Title
Contextualizing Institutional IT Policy: A Historical Narrative of UCLA’s Policymaking Environment

Permalink
https://escholarship.org/uc/item/0160r7kr

Author
Chamberland, Kristen

Publication Date
2016

Peer reviewed|Thesis/dissertation
Contextualizing Institutional IT Policy:
A Historical Narrative of UCLA’s Policymaking Environment

A dissertation submitted in partial satisfaction of the requirements for the degree of Doctor of Philosophy in Information Studies

by

Kristen Marie Chamberland

2016
ABSTRACT OF THE DISSERTATION

Contextualizing Institutional IT Policy:
A Historical Narrative of Information Technology Policy at UCLA

by

Kristen Marie Chamberland

Doctor of Philosophy in Information Studies
University of California, Los Angeles, 2016
Professor Leah A. Lievrouw, Chair

Information technology (IT) policymaking in higher education is often an ad hoc process, responding to crises, rather than taking a proactive approach based on a clear understanding of the policy environment, resulting in inconsistency, inefficiency, and confusion. Without sufficient contextualization, university IT policy lacks the vision and comprehensive strategy needed to ensure its effectiveness and durability. Through a historical narrative of three cases of recent IT policy events at UCLA, this dissertation examines the features of the institutional policy context that shape technology policy development. By tracing the cases studies’ events and shared themes of academic freedom, free inquiry, information privacy, information security, data protection, and peer-to-peer digital piracy, the study demonstrates the complexity of the policy context and its changes over time. To guide policy research and writing, it draws from the historical case study data and proposes an analytical framework based on three prominent contextual elements--institutional values, governance, and stakeholder relationships. By applying
that framework to recent and emerging IT policy issues at UCLA, the paper demonstrates the usefulness of a structured informed approach to complex institutional IT decision-making.
The dissertation of Kristen Marie Chamberland is approved.

Jonathan Furner
Christopher M. Kelty
James Davis
Leah A. Lievrouw, Committee Chair

University of California, Los Angeles
2016
To Raymond and Mary Chamberland,

who dared me to ask questions and supported my every endeavor to answer them.
# TABLE OF CONTENTS

List of Figures ........................................................................................................... x

Glossary ....................................................................................................................... xi

Curriculum Vitae .......................................................................................................... xiii

Chapter 1 Introduction ............................................................................................... 1
  Overview ..................................................................................................................... 1
  Major Themes in Institutional IT Policy Studies ....................................................... 2
    Institutional/Organizational Culture Studies ......................................................... 2
    Institutional Climate Studies .............................................................................. 4
    Infrastructure Studies ......................................................................................... 5
  Key Concepts in IT Policy Contextualization .......................................................... 8
    Institutional Values .............................................................................................. 8
    Governance Structures and Processes ................................................................. 10
    Stakeholder Relationships ................................................................................. 11

Methods ....................................................................................................................... 12
  Study Setting ............................................................................................................ 12
  Author as Insider ..................................................................................................... 13
  Case Studies ............................................................................................................ 14
  Limitations of the Study ......................................................................................... 17
  Application to other institutions ............................................................................ 17

Conclusion ................................................................................................................... 18

Chapter 2 The Expression of UCLA’s Institutional Values: University of California’s
  Electronic Communications Policy ........................................................................... 19
  Overview ................................................................................................................... 19
  Background .............................................................................................................. 20
  Information Technology Challenges the University Mission ............................... 22
    University of California’s Response to the Challenges ....................................... 23
  The Roots of the ECP, 1960s–1990s .................................................................... 25
    Electronic Mail and the ECPs Predecessors, 1990s ............................................ 27
  Developing the ECP, 2000–2005 ......................................................................... 30
    The ECP’s Provisions ........................................................................................ 30
    Related Policies .................................................................................................. 33
  Revising the ECP 2005–2011 ............................................................................... 33
  Implementing the ECP at UCLA ......................................................................... 36
    Acceptable Use ................................................................................................... 37
    Privacy and Confidentiality ............................................................................... 37
    Security ............................................................................................................... 38
    Retention and Disposition ............................................................................... 39
  Values Embodied in UCLA’s Policies and Practices ......................................... 39
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Principles</td>
<td>39</td>
</tr>
<tr>
<td>Academic Freedom</td>
<td>40</td>
</tr>
<tr>
<td>Privacy and Confidentiality</td>
<td>41</td>
</tr>
<tr>
<td>Security</td>
<td>44</td>
</tr>
<tr>
<td>Balancing Values in UCLA’s Information Technology Policy</td>
<td>46</td>
</tr>
<tr>
<td>Balancing Privacy, Transparency, and Efficiency</td>
<td>47</td>
</tr>
<tr>
<td>Balancing Privacy and Security</td>
<td>49</td>
</tr>
<tr>
<td>Advantages and Drawbacks of the Balancing Test</td>
<td>51</td>
</tr>
<tr>
<td>Potential Future Challenges to UCLA’s Approach</td>
<td>52</td>
</tr>
<tr>
<td>Maintaining a Principled Position</td>
<td>53</td>
</tr>
<tr>
<td>Cloud Computing and External Vendors</td>
<td>55</td>
</tr>
<tr>
<td>Conclusion</td>
<td>60</td>
</tr>
</tbody>
</table>

Chapter 3 UCLA’s Governance Structure at Work UCLA Advisory Board on Privacy and Data Protection | 62 |
| Overview                                                               | 62   |
| Background                                                             | 63   |
| UCLA’s Shared IT Governance                                           | 65   |
| Values in Practice                                                     | 68   |
| The Privacy Board’s Inception                                         | 72   |
| Emerging Technology Challenges Privacy Values                          | 72   |
| Proposing the Board to the ITPB                                       | 75   |
| The ITPB’s Recommendation                                              | 77   |
| The Privacy Board’s Charge                                             | 77   |
| The Charge                                                             | 77   |
| Membership                                                             | 78   |
| The Board’s Role in UCLA’s Governance Structure                        | 80   |
| Scope and Scale                                                        | 82   |
| Perceptions of Early Successes and Failures                            | 82   |
| Key Operational Issues                                                 | 83   |
| Illegal File-sharing                                                   | 84   |
| Privacy and Academic Freedom in Research                               | 84   |
| The Data Security Breach                                               | 85   |
| Contracting Cloud Services                                             | 85   |
| Opus                                                                   | 87   |
| Restructuring the Board                                               | 89   |
| The Visionary Mission                                                  | 91   |
| Developing Privacy Principles                                         | 91   |
| Value-Based Language in the Privacy Principles                         | 93   |
| Guidance for Individuals                                              | 95   |
| UCLA’s Leadership Role in the UC Privacy Initiative                    | 96   |
| UC’s Steering Committee                                                | 96   |
| Charge and Goals                                                       | 96   |
| Localization                                                           | 100  |
| UCLA’s IT Governance Landscape                                        | 100  |
| Looking Forward: Challenges to IT Governance                           | 103  |
| Data Deluge and the Evolution of Data Protection                       | 103  |
| IT’s New Challenges                                                    | 104  |
Chapter 4 UCLA’s Stakeholder Relationships Implementing the DMCA on Campus... 114
Overview .................................................................................. 114
Background ................................................................................ 115
Stakeholders .............................................................................. 119
UCLA Fields Infringement Claims ............................................. 120
Policy 464 .................................................................................. 120
An Infringement Notice Influx .................................................. 121
Standing Up to Industry Stakeholders ...................................... 123
UCLA’s Hollywood Connections ................................................. 123
Attempts at Cooperation .......................................................... 125
Institutional Research as a Stakeholder Bridge ......................... 127
UCLA Builds a Holistic Strategy ............................................... 129
Testifying Before Legislative Stakeholders ............................ 129
DMCA Strategy Step 1: Quarantine ........................................... 130
Notification and Acknowledgement ......................................... 131
Proposed Quarantine Software ................................................. 132
DMCA Strategy Step 2: Offering Legal Alternatives ............... 134
DMCA Strategy Step 3: Educational Outreach ......................... 135
Outreach .................................................................................... 136
Workshops ................................................................................ 137
Balancing Multiple Stakeholder Interests ................................ 139
A Holistic Approach to Multiple Interests .............................. 139
Recognizing a Technology Issue as a Societal Issue ......... 140
Societal Good and Citizen Building ........................................ 141
UCLA as a Teacher and Leader ............................................... 142
Looking Forward—DMCA Strategy Reapplied ...................... 143
Instructional Materials—UCLA Resists External Pressure .... 143
Course Websites—UCLA Teaches Copyright ........................... 145
Conclusion ................................................................................ 146

Chapter 5 An Analytical Framework for Policy Contextualization .... 148
Historical Narrative as Policy Context .................................... 148
Framing IT Policy Context ........................................................ 149
The Importance of UCLA’s Mission and Values .................... 150
UCLA’s Scale and Scope ........................................................... 151
A Holistic Approach to IT Policy and Issues .......................... 153
Addressing Multiple Interests ................................................. 153
Bottom-Up Policymaking ......................................................... 155
Holistic Approaches in the Policy Context Framework .......... 157
Teachable Moments in the Holistic Approach ....................... 159
Applying the Policy Context Framework to Emerging IT Policy Issues 165
UCLA’s Online Education Initiative ........................................ 166
UCLA Heath System’s Cyber Attack ....................................... 171
Conclusion ................................................................................ 174
LIST OF FIGURES

Figure 1: Institutional culture and IT infrastructure overlap ........................................7
Figure 2: Privacy types ........................................................................................................69
Figure 3: UCLA Privacy Board's authority and relationships ..............................................81
Figure 4: Policy context framework ..................................................................................149
Figure 5: The holistic approach in the policy context framework .....................................154
Figure 6: Examples of teachable moments in the policy context framework .................160
GLOSSARY

AIME Association for Information Media and Equipment
BAYU Be Aware You’re Uploading
BYOD bring your own device
CCLE Common Collaboration and Learning Environment
CISCO Chief Information and Security Officer
CPO Chief Privacy Officer
CPRA California Public Records Act
DMCA Digital Millennium Copyright Act
DRM Digital Rights Management
ECP University of California’s Electronic Communications Policy
FERPA Family Educational Rights and Privacy Act
GSE&IS Graduate School of Education and Information Studies
HIPAA Health Insurance Portability and Accountability Act
IP Internet protocol
IRB Institutional Review Board
ISP Internet service provider
IT information technology
ITPB Information Technology Planning Board
LMS Learning Management System
MPAA Motion Picture Association of America
OECD Organisation for Economic Co-operation and Development
OIT Office of Information Technology
P2P peer-to-peer

RIAA Recording Industry Association of America

UC University of California

UCLA University of California, Los Angeles
CURRICULUM VITAE

EDUCATION

BA in History and Philosophy 2002
Loyola Marymount University

PROFESSIONAL EMPLOYMENT

Programmer/Analyst III 2010-present
Educational Technology Unit, UCLA Graduate School of Education and Information Studies
• Manage and develop graduate and undergraduate instructional technology resources
• Administer streaming media services and video capture/editing/encoding workflows
• Administer and support UCLA’s Learning Management System
• Administer school website and cloud storage and archive services

Consultant 2015
Office of Information Technology, UCLA
• Consulted with UCLA’s Chief Privacy Officer to revise UCLA’s information technology policies to ensure compliance with University of California policy

Lecturer 2005-2006
Université de Rouen
• Instructed undergraduate courses in English and American culture.
• Consultant to Cercles, an Anglophone scholarly journal

Programmer/Analyst I, II 2002-2010
Educational Technology Unit, UCLA Graduate School of Education and Information Studies
• Provided end-user support to faculty, staff, students for Apple hardware, software, network homes, server spaces, remote connections. Hardware and software installation, upgrade, purchasing.
• Instructed ED 301, teaching video capture, editing, compression and creating digital education materials
• Managed a multimedia classroom to develop distance learning and streaming media

UNIVERSITY SERVICE

CCLE Standards and Practices Group 2015-present
UCLA Data Governance Task Force 2015-2016
UCLA Advisory Board on Privacy and Data Protection 2014
GSE&IS Information Technology Advisory Committee, Chair 2013-present
CSG Streaming Media and Storage Subcommittee, Chair 2015-2016
UCLA Media Casting Coordinators Committee 2008-2015
CHAPTER 1
INTRODUCTION

Overview

Information technology (IT) policymaking in higher education is often an ad hoc process, proceeding from crisis to crisis. That process takes place in an institutional context that is shaped by many cultural and technological forces, some more visible than others. The purpose of this project is to answer the question, “What are the features of the policy context at UCLA and how has it shaped the development of IT policy?” To answer this question, my goal is to propose a more systematic account of IT policy development, based on a historical analysis of recent IT policy at UCLA. The analysis focuses mainly on three critical IT developments at the university between 1998 and the present: The Electronic Communications Policy, UCLA’s Advisory Board on Privacy and Data Protection, and the university’s response to the Digital Millennium Copyright Act.

Employing the three events as case studies, I construct a historical narrative in the context of institutional IT policy at UCLA with a focus on three key mutually determining aspects that emerged from my analysis: institutional values, governance, and stakeholders. Together, the three elements can be used as an analytic framework to study the institutional context and explore processes by which administrators conceptualize, write, and implement IT policy and possibly apply to future IT policy developments.

This study contributes to the field of information studies by leveraging oral history and document analysis to better understand how institutional culture and IT infrastructure shapes IT policymaking. Secondarily, it contributes to science and technology studies research by
analyzing the IT policy-making process as a system of interconnected institutional dynamics that shape academic IT resources.

**Major Themes in Institutional IT Policy Studies**

Several disciplines have contributed to the understanding of IT policy development in higher education, including institutional/organizational culture and climate studies, and infrastructure studies in fields ranging from business to sociology and psychology. Likewise, multiple disciplines ground this study’s theory and inform its qualitative approach.

**Institutional/Organizational Culture Studies**

At the most basic level, institutions create and implement policy within an institutional context. The broad and well-established literature on institutional culture is a useful point of departure for thinking about institutional context. Kuh and Witt, for example, provided a succinct definition of institutional culture:

> [T]he collective, mutually supporting patterns of norms, values, practices, beliefs, and assumptions that guide the behavior of individuals and groups in an institution of higher education and provide a frame of reference within which to interpret the meaning of events and actions on and off campus. (1988, p. 7)

It is helpful to think of an institution as a system. The pervasiveness of institutional culture is noted in nearly every definition in the literature. Bitzer points out that institutional culture is ubiquitous; “[E]very organization, every department, and even every little informal work team has a culture.” The presence of culture indicates that institutions are “living and changeable entities, as are the people who comprise them” (2009, p. 335). Joseph Simone proposes a similar definition: it is the “common ideas, values, and standards that permeate the everyday lives of its members, and that are perpetuated by institutional indoctrination, actions, and leadership” (2009, p. 5). The authors of a 2005 ASHE report describe it as being “deeply embedded within an
organization, distinctive to it, and enduring, thus providing identity and meaning for its members” (“ASHE Higher Education Report: Special Issue: The Uses of Institutional Culture: Strengthening Identification and Building Brand Equity in Higher Education,” 2005, p. 40)

It is also helpful to think of institutional cultures as dynamic systems. Studies of institutional/organizational culture often point out that culture is not static, but a dynamic process that guides, binds, provides, expresses, and forms identity. Institutional culture facilitates commitment, enhances stability, guides sense-making, and defines authority. It combines diverse elements of an organization into a whole and provides a frame of reference that allows members to interpret the meaning of events. An institutional culture’s ability to confer identity on its members is a critical function. The ASHE report, building upon Kuh and Witt’s (1988) themes, explains,

At universities and colleges, institutional culture conveys a sense of identity (who we are), facilitates commitment (what we stand for), enhances stability (how we do things around here), guides sense making (how we understand events), and defines authority (who is influential). (“ASHE Higher Education Report: Special Issue: The Uses of Institutional Culture: Strengthening Identification and Building Brand Equity in Higher Education,” 2005, p. 5)

There are several forms of institutional culture; the ASHE report distinguishes four common elements: symbols, language, narrative, and practices. All institutions have them, yet they are distinct to each, giving form to the norms, values, and beliefs. Symbols are the most common form of institutional culture in universities: colors, logos, mascots, ceremonies, robes, and mottos are all common symbols that convey varying degrees of strength, camaraderie, reliability, and timelessness. Language, which conveys symbols, is an important form of culture for this study: the terminology, phrasing, and use of jargon in policy are important indicators of the culture in which it was written. Narratives, which encompass “myths, legends, sagas, and stories,” are the building blocks of institutional memory. Practices, described by the authors as
“rituals, rites, and ceremonies” also include day-to-day interactions among researchers, coworkers, faculty groups, students, and administrators. The degree of formality, flexibility, inclusiveness, record keeping, and adherence to hierarchical structure are all important aspects of institutional culture for this study.

Payne (2001) proposed further options for studying organizational culture and change. Payne created a three-dimensional framework to analyze culture, assessing strength of any given culture based on a 5-point scale of managerial influence. Although the scaling approach is more formal than the explanatory approach of the present project, Payne’s identifiers are helpful ways to think about aspects of culture. The author first assessed the degree of consensus among members, from high to low; second, measured the pervasiveness (the range of behaviors imposed on the group) from narrow to wide; and last, assessed psychological intensity (which manifests as “taken-for-granted assumptions or unconscious beliefs”) from deep to shallow. The resulting “Culture Cube,” the factors of how members may internalize forms of institutional culture. In addition, Payne described criteria for measuring the process of change in culture, which can also be adapted to design useful questions about how institutional culture changes (2001, p. 108).

Institutional Climate Studies

“Climate” has been used as a metaphor for framing, organizational and institutional cultures and contexts. Definitions of climate differ across disciplines and often intersect or are used interchangeably with concepts of institutional/organizational culture. However, the term “climate” has often been used to suggest a factor that can be assessed quantitatively to contextualize organizational phenomena such as achievement, productivity, and morale.

In the late 1970s and 1980s, many researchers employed the organizational climate concept, but its use was hotly contested. Moran and Volwein (1988) cited dozens of studies, with contradictory definitions and results, which muddied the concept. However, many researchers
considered it a useful way to understand the relationships among individuals in an organization, and because of the need to assess performance and behavior, and the desire to create effective models for organizational development, the concept of continues to be used (Moran & Volkwein, 1988).

Later discussions singled out parts of the original definition of climate and redefined them as culture (Davey & Symon, 2001; Kuh & Whitt, 1988; McMurray & Scott, 2003; Payne, 2001; WASC Committee, Department of Academic Affairs, 2000). These researchers differentiated between climate and culture, and conceptualized them simultaneously in the organization. Although different authors’ views have varied on specific aspects, the idea that climate relates to demographics and can be measured quantitatively, whereas culture is assessed qualitatively, seems to be the standard. For example, researchers often describe climate as positive or negative, and culture as strong or weak.

**Infrastructure Studies**

An institution’s policy context is also based on it technology infrastructure. Recent scholarship in the emerging field of infrastructure studies is also instructive in this regard. IT infrastructure comprises the essential elements of the environment that facilitate computing and communications. In higher education, it is the foundation for digital communication, information sharing, research, and instruction. It serves the educational mission by allowing access to electronic information, providing resources for creating and processing data, and facilitating collaboration in the university community.

Traditionally, infrastructure has been understood as the physical facilities and systems in a city or nation, such as roads, bridges, public transportation, water, power, and telephone systems. Information technology is layered in over existing infrastructure. Hardware adds a layer of cables, wires, fiber, routers, hubs, servers, personal computers and terminals, and wireless
devices. Software adds another layer of network and computer operating systems, communications protocols, programming languages and communication interfaces, directories and repositories. Together, the layers consist of “ensembles of things (e.g. pipes, wires, and servers) that connect or transport people, fluids, signals, and such” (Karasti, Baker, & Millerand, 2010, pp. 381–382). Edwards, Bowker, Jackson, and Williams (2009) note that in the 1990s, “the information superhighway metaphor deliberately coupled the older hardware of urban civilization to rapid digital convergence” (2009, p. 365). Put simply, it is a “broad category referring to pervasive enabling resources.”

But science and technology studies (STS) scholars have advanced an even more inclusive notion of infrastructure, including not only hard assets, but also human, process, and organizational elements (Bowker, Baker, Millerand, & Ribes, 2009). Karasti, Baker, and Millerand (2010) describe the elements as the “interrelated technical, social and organization arrangements involving hardware and software technologies, standards, procedures, practices and policies together with digital configurations in support of human communication and capabilities” (2010, p. 380). Bowker et al. argue that people and systems are as vital for information handling as hardware and protocols (Bowker et al., 2009, p. 103). Here, intentionally blurring the line between technological infrastructure and organizational infrastructure allows for a more holistic theory.

Star and Ruhleder (1996) noted that conventionally, infrastructure is understood as something that runs in the background and only becomes visible in the case of breakdown. They argue that this conceptualization is “neither useful or accurate,” and argue instead that infrastructure is a “fundamentally relational concept” whose degree of visibility depends on context. They use the example of a water system, which is essential infrastructure to a cook, but “a variable in a complex system” to a city planner. Thus, infrastructure is not a what but a when
Bowker et al. assert that an expanded conceptualization can “better take into account the social and organizational dimensions of infrastructure” and consider it “not only in terms of human versus technological elements but in terms of a set of interrelated social, organizational, and technical components or systems” (2009, p. 98).

Based on this brief overview of concepts related to the institutional context of IT policymaking, the main points can be summarized and related, as depicted in Figure 1.

![Venn Diagram](image)

**Figure 1:** Institutional culture and IT infrastructure overlap

Cultural factors are represented in the circle on the left, and infrastructural factors in the circle on the right. The Venn diagram-type area of overlap represents the practices of the people in the institution that are shaped by factors from both sides, including faculty, academic administrators, students, and staff.

IT employees are an essential part of the institutional culture, with their own values, rights, and expectations. They are integral to IT infrastructure as well by managing technology implementation, maintenance, troubleshooting, and training. They set and follow standards, and develop common practice. Their time, capabilities, and dedication both enable and limit
technology usage by other campus members. Resources allocated for support staff is an indication of priorities within the policy context; for instance, the investment in experienced or talented staff is indicative of the dedication to cutting-edge (or at least current and consistent) services. But the reality of the support staff’s ability to provide services shapes infrastructure as much as the physical technology. IT does not appear or evolve on its own; it must be built, operated, managed, and governed by knowledgeable people. Thus, in the present study there has been a particular focus on the experience and practices of the people involved in IT policy at UCLA.

Key Concepts in IT Policy Contextualization

Three essential themes emerged from case study analysis in this project. As I investigated each of the three UCLA IT policy cases, I noticed three repeated themes—institutional values, governance, and stakeholder relationships. Each of the three had a different prevailing theme, as identified in Chapters 2-4. But it is important to note that they are present in each case, intersecting at various points in the narrative. In Chapter 5, I will discuss my interpretation of the elements’ interconnected relationships.

Institutional Values

Values are judgments of importance; in this context they are the deeply held ideals and priorities of a collective. Calder explains values as the “underlying assumptions that influence the institution’s activities” (Calder, 2014, para. 7). He argues, “when [the institution’s] values are deeply entrenched and widely shared by stakeholders, the institution’s culture of values soon becomes a way of life in the workplace which shapes an institution’s strategic intentions” (2014, para. 9). Values are the basis for institutional members’ concepts of rights, expectations, and intentions.
UCLA lays out its ideology in its mission statement. UCLA stakeholders stated their purpose to be rooted in the “creation, dissemination, preservation, and application of knowledge for the betterment of our global society” (UCLA, n.d.-b). Stakeholders at UCLA have a keen interest in protecting their First Amendment rights, especially as they relate to academic freedom. Academic freedom ensures faculty and students the ability to “engage in intellectual debate without fear of censorship or retaliation.” It allows students and faculty to research the topics they choose, and allows them to express their views “in speech, writing, and through electronic communications, both on and off campus” (Nelson, 2010, para. 2-6). Academic freedom is an umbrella term that covers a cluster of more basic values, including free speech, free inquiry, and knowledge sharing. Because it protects electronic communications, it includes IT-specific values such as information privacy, security, and data protection.

UCLA’s mission statement expresses a commitment to academic freedom “in its fullest terms.” Other values detailed in the mission statement include the importance of knowledge production, teaching and learning, social justice, and civic engagement. Institutional values provide principled guidance to decision-making processes. Though UCLA may choose to interpret those values differently over time, university policy tends to be most consistent the closer it remains to original intent.

The ASHE report theorizes the role of values in institutional culture, based on the founding mission of the school, which differs among institutions. Depending on the values of the founding body (duty to the state, religion, military, politics, etc.), some universities value instruction above all else, whereas others focus on research and knowledge production. Some share commitment to socioeconomic diversity or community engagement, assuming these values directly influence the culture of the university, but do not provide further analysis. UCLA’s
mission statement states that its “primary purpose as a public research university is the creation, dissemination, preservation and application of knowledge for the betterment of our global society.” Also listed in the statement are commitments to diversity, innovation, and civic engagement. The sweeping goals of this statement, while noble, vary markedly, causing the reality of obtaining each element unlikely, if not impossible. But neither should the values be discounted: the resistance to limitations on focus are evident in some policies as well as day-to-day experiences on campus. Chapter 2 will provide further examination of the role of values, goals, and mission in the policy context at UCLA.

**Governance Structures and Processes**

Theories of governance have spread beyond governments to institutions, corporations, and even informal organizations. Thus, as Bevir explained, governance refers to:

> All processes of governing, whether undertaken by a government, market, or network, whether a family, tribe, formal or informal organization, or territory and whether through laws, norms, power, or language. Governance differs from government in that it focuses less on the state and its institutions and more on social practices and activities. (2012, p. 3)

This study examines governance in two senses: the structures, which are the decision-making bodies, and the processes, the actions taken by governing individuals or bodies, such as policy writing, implementation, and enforcement. Institutional governance bodies provide leadership and strategy by setting the organization’s goals, responsibilities, and accountability. Theoretically, governance structures frame and structure the work, and are distinct from management, which organizes the work, and operations, which carries out the work. In public institutions, governance is associated with democratic participation.

The UCLA’s Office of Information Technology (OIT) states that the IT governance mission is to “ensure that UCLA’s IT capabilities continue to sustain and extend its strategies and objectives.” Its goals include (a) integrating IT strategic planning with campus strategic
planning, (b) accounting for IT initiatives, (c) providing transparency for IT plans and investments, (d) adopting a broad campus-wide view, (e) sharing and using IT best practices, (f) encouraging entrepreneurial spirit and creativity in applying IT, and (g) encouraging active participation in the IT governance process (UCLA, n.d.-a). It attempts those goals through a combination of “leaderships, organizational structures, and processes.”

UCLA’s IT governance structure consists of three governance committees, which act in consultation with several others. The Information Technology Planning Board (ITPB) consists of administrators and the Academic Senate faculty makes strategy and policy recommendations. The Committee on Information Technology Infrastructure, whose members include appointed academic and administrative directors, conducts tactical planning, operational policy, business modeling, and budgeting. The Common Systems Group coordinates central and distributed IT activities around campus; representatives include IT directors and technology administrators. The OIT manages technology governance.

UC and UCLA operate under a shared governance model, meaning that oversight and decision-making responsibilities are distributed between administrators and faculty. The model ensures that faculty interests, particularly those related to academic freedom, are served along with administrative needs. It allows the university to balance the issues of multiple stakeholders and serve a multi-part mission, as discussed further in Chapter 3.

**Stakeholder Relationships**

As defined by Maric, stakeholders are “any group or individual who can affect or is affected by the achievement of the organization objectives.” They include any constituencies in the organization’s external environment that are affected by the organisation’s decisions and actions” (Maric, 2013, p. 222). In the United States, typical stakeholders in public higher education institutions are both internal and external: students, parents, faculty, staff, governing
bodies, private industry, and local communities. Analyzing the relationships and relative priorities among university stakeholders provides clues to the dynamic nature of policy context.

This study analyzes the ways in which public and private sectors’ interests intersect, and how stakeholders communicate. Despite being a public institution, UCLA has strong ties to the entertainment industry. External interests influence intellectual property issues, and at UCLA, those interests are literally down the street. Perhaps more than any other content creator, the entertainment industry has supported and benefited from intellectual property law, particularly the DMCA. However, educational institutions have a stake in intellectual property issues as well; they rely on intellectual property exceptions for instructional purposes. When the DMCA indiscriminately blocked access to digital content, educational institutions were unable to exercise their fair-use rights. This study examines interactions between UCLA and the entertainment industry to highlight the significance of external stakeholders in the policy context, the focus of Chapter 4.

Stakeholder roles in policy discussions are dynamic. For instance, the UC system’s stakeholdership can be considered internal or external, depending on the situation. Interview participants refer to the UC System, the Regents, and the Office of the President as “we” when they agree with the UCLA campus, and as “them” when they do not.

Methods

Study Setting

UCLA is an ideal setting for this study, for several reasons. The university is an integral part of the UC system, with the largest student enrollment of all UC campuses and second largest endowment. In IT, UCLA’s history as the first node of Advanced Research Projects Agency Network (ARPANET) qualifies it as a forerunner in the origins of the Internet (Federal
Communication Commission, 2005), and UCLA’s professed ongoing commitment to digital technologies makes the initial contribution significant. Continued campus-wide technology implementation in the wake of that national prominence suggests that UCLA is committed to keeping its place at the cutting edge of development. Although UCLA’s history may be somewhat unique in this regard, it has contributed to the and institutional mission devoted to knowledge production, instruction, and community service, which goals shared by many U.S. higher education institutions, but major commitments at UCLA. Also, part of UCLA’s role is service to the state of California, it has this public interest commitment in common with public universities.

Author as Insider

UCLA is also a logistically ideal study setting, given my own professional role. I have been employed as a technician at the Graduate School of Education and Information Studies (GSE&IS) since 2002 and a student since 2008. My roles as student and staff member give me a unique perspective and array of access opportunities, and my familiarity with technology administration and support on campus allows for a nuanced interpretation of events on campus. In my position as a Programmer/Analyst, I have participated in various decision-making entities, including the Instructional Enhancement Initiative implementation group, Common Collaborative Learning Environment (CCLE) administration, Media Casting Coordinators, GSE&IS’ Information Technology Advisory Committee and chaired an inquiry committee for the Common Systems Group. I served as a graduate student representative on the Advisory Board for Privacy and Data Protection and the Data Governance Task Force. Technology committees at UCLA have many overlapping members, so the relationships I have built through my work aided my research by establishing trust and a sense of familiarity and shared
stakeholdership. Many of those faculty and IT employees agreed to participate in my data-gathering process.

**Case Studies**

Through a set of historical case studies, this study assesses how UCLA’s IT policy environment has developed over time, and key themes for factors within that development. There were two sources of data for the cases: documents generated by various university units and personnel responsible for IT development at UCLA, and interviews with key individuals involved in the campus’ IT decision-making (faculty, administrators, and technical staff.) Initially, I conducted informal, unstructured interviews with five IT support colleagues, inquiring about the validity of the notion that UCLA’s IT policy differed from other universities. Each agreed with the claim, and gave a few examples, such as a respect for information privacy, a commitment to academic freedom, faculty inclusion in decision-making, and UCLA’s relationship with the entertainment industry. A few common themes surfaced in their examples: cooperation and collaboration, decentralization, balance, and competition, which I noted as potential categories for my initial analysis.

From these discussions with my initial contacts, three significant IT-related events in UCLA’s past emerged as “milestones” in the evolution of the IT policy-making context. The first was UC’s establishment of the ECP in 2000 and UCLA’s subsequent implementation. The second was the establishment of the UCLA Advisory Board on Privacy and Data Protection in 2004. The third was UCLA’s response to the Digital Millennium Copyright Act (DMCA), enacted by Congress in 1998. These milestones represented nearly two decades of technological innovation and oversight, and suggested a common narrative with a few main themes. Each has had a broad impact on UCLA’s institutional culture, and the deeply-rooted set of norms, values, practices, and beliefs held by members of the institution. IT policies influence and are influenced
by beliefs and behaviors that guide daily life on campus, as well as long-term commitments to
the university’s stated goals and missions that guided its research, instruction, and community
relationships. In all three cases, students, staff, and faculty were using the technologies in
question. Additionally, integral parts of the UCLA mission were impacted, including research,
instruction, and the relationship with the community. Each policy milestone transpired over a
span of several years, and involved continual revisions, changes, and adaptation. The cases also
fit into a national context, allowing for an investigation of UCLA’s IT policy in a broader scope.
Policy development in each case reflected corresponding fluctuations in the institution’s policy
context over time.

I drew on a mixture of sources to investigate these cases. In interviews conducted over
approximately nine months beginning in 2013 (with select follow-ups from 2014 through the
spring of 2016), I collected the perspectives of eight key UCLA faculty, administrators, and IT
staff. I concentrated on decision-makers and committee members most closely involved in IT
policy. I recorded the audio from each 60 to 90-minute interview, while taking field notes
regarding my participants’ affect and inflection. At some points, I asked for details about time,
organization names, titles, and participants, but I left questions open ended and encouraged
interviewees to tell their own stories and share their views. With the flexible format, it was more
difficult to construct a comprehensive narrative, but it enabled a richer interpretation of UCLA’s
institutional culture and policy context. I determined that knowing precisely what happened was
secondary to gaining insight into how and why it did.

As a state institution, UCLA (like the UC as a whole) routinely publishes documents
relating to all aspects of its operations, including IT policy and services. UCLA classifies IT-
related policy documents numerically, and makes them available online, as well as committees’
founding documents, agendas, notes, drafts, and published statements. In addition, I was able to locate and compare previous versions of policies and draft documents to trace policy development through those revisions. I interpreted tone, content, and timeline in supplementary documents including letters, internal memoranda, position statements, and campus news. These sources helped establish the narrative’s foundation and gave clues about the cultural context in which they were written.

I collected both interviews and documents simultaneously; I found potential interview candidates mentioned in documents and by other interviewees. Interviewees often also recommended documents related to their recollections. I transcribed each interview and transferred them along with field notes and documents to qualitative analysis software for coding, beginning with the initial categories mentioned above: cooperation and collaboration, decentralization, balance, and competition. From there, I conducted a thematic textual analysis and constructed a timeline of events. During the analysis stages, viewing my historical data through the initial categories led me to discover more substantial and relevant first-level themes (values, governance, and stakeholder relationships), with the categories reorganized as sub-themes.

In the following chapters, the three cases are presented in order of scope, from broad to narrow. The UC’s Electronic Communications Policy (ECP) case is the most far-reaching case, affecting ever aspect of IT policy at UCLA and the whole UC. The Advisory Board on Privacy and Data Protection (hereafter referred to as the Privacy Board, its common name) was created with the specific belief of advising on data protection and privacy issues on campus, though its purview gradually expanded to touch on virtually all IT policy at UCLA. The DMCA case was

---

1 UCLA’s Administrative Policies and Procedures are available online. Information Technology is Subject Area 4; all IT-related policies are numbered in the 400s. http://www.adminpolicies.ucla.edu/subjectarea/Default.aspx?&subjectarea=4
the narrowest, dealing just with intellectual property infringement, though it gradually became a touchstone for the campus’ emphasis on “teachable moments” arising from policy violation.

**Limitations of the Study**

When I formulated this project, I assumed that I would encounter some resistance from my interviewees on controversial topics. Instead, my subjects were amenable, but tended to express themselves with remarkably consistent terms and positions. It was difficult to ascertain if they were sharing personal perspectives, or were instead presenting a unified front (despite the promise of anonymity). I suspect I heard both; perhaps they had internalized fundamental concepts that then affected subsequent viewpoints. In my open ended interviews, I attempted to lead the discussion minimally, but oral histories are always shaped to some degree by historians’ assumptions. Relying on interviewee’s memories limited my ability to construct a complete narrative; my participants had many stories to share about Privacy Board and DMCA cases, but they relayed mostly facts about the early days of the ECP. Limitations occurred as a result of my documentary sources as well. Some previous policy versions are unavailable, necessitating assumptions and interviewees’ accounts to bridge the gaps.

**Application to other Institutions**

The case study findings may not apply directly to other universities; a common theme in each case was UCLA’s unique policy approach. UCLA tends to privilege academic freedom, resulting in different solutions to common technical issues than are typical at other institutions. But a three-part mission of instruction, research, and service is a common model in higher education institutions; universities may fulfill them differently, but the foundation is the same. The case study approach here might also be adapted to studies of other institutions, although other events or milestones might be more relevant elsewhere.
Conclusion

The institutional policy context for institutional decision-making is the metaphorical environment in which policy decisions are made and created and implemented. My research question asks how policy-making can best be understood in context. I began my exploration of UCLA’s context with broad ideas about institutional culture, drawn from a range of literatures, and with the aim of constructing a historical narrative. Utilizing a blend of document analysis and oral history methods, I examined decision-making processes within the institution, and its resulting policy and implementation. In the following chapters, I describe how and why each event emerged as a critical IT policy issue, and suggest major themes that emerged in each case during my analysis. The chapters’ cases are characterized by a single theme, but at several points I highlight the intersection and interplay of multiple themes as they occurred in the narrative. In the concluding chapter I propose connections among those themes, as a tentative analytic framework for thinking about the process of IT policy development in higher education.
CHAPTER 2
THE EXPRESSION OF UCLA’S INSTITUTIONAL VALUES:
UNIVERSITY OF CALIFORNIA’S ELECTRONIC COMMUNICATIONS POLICY

Overview

The way the UC system and UCLA writes, interprets, and implements policy reflects institutional values, which are an important part of the IT policy context. Through policy, values speak to technology’s role in the educational mission. UCLA’s mission draws heavily on academic freedom values, which are simple in theory, but challenging to practice consistently institution-wide.

In this chapter, I present a case study of the ECP to illustrate that while values are key to the institution, they are varied and can conflict as much as the various interests they reflect. The ECP exemplifies UC and UCLA using policy to protect core academic values by ensuring the safety and confidentiality of its members’ communications. The ECP is the crystallized value statement of the UC system. The ECP applies systemwide, but each UC campus must provide local implementation. At UCLA, the ECP and its related policies articulate institutional values through practice (UC Office of the President, 2000).

In this chapter, I explore several layers of institutional values in the context of one of the university’s most significant technology policies. While examining the ECP and its interpretation and implementation at UCLA, I argue that this case aptly represents the negotiation of values consistent with UCLA’s other IT policies. The ECP case establishes the prominence of values in the university’s IT decision making and establishes fundamental concepts frequently referenced in the following two cases. This chapter opens with a brief overview of the policy and the
institutional values it represents, then explores preceding policies and the ECP’s development over time. To narrate this, I include recollections from UCLA administrators, IT support staff, and faculty members who were part of shaping the ECP at UCLA. Then I map the system of interconnected policies at UC and UCLA to evaluate the relationship between values and policy implementation. I conclude with a discussion of the technological advances and changing institutional needs challenging current policies and practices.

**Background**

UC and UCLA share a three-part mission of education, research, and public service. The mission combines a public institution’s values and responsibilities. UCLA’s mission statement identifies academic freedom as a necessary foundation:

UCLA’s primary purpose as a public research university is the creation, dissemination, preservation, and application of knowledge for the betterment of our global society. To fulfill this mission, UCLA is committed to academic freedom in its fullest terms: We value open access to information, free and lively debate conducted with mutual respect for individuals, and freedom from intolerance. (UCLA, n.d.-b)

As mentioned in Chapter 1, academic freedom is a doctrine allowing scholars to inquire freely about topics without institutional constraints or governmental censorship. Its principles protect scholars’ abilities to research any topic, have open discussions in classrooms, and publish on controversial topics without fear of reprisal.

People may be inhibited from doing their best work if they fear offending outside forces, such as politicians or donors, inside authorities, such as trustees or senior administrators. Without academic freedom, our society would lose professors’ best inventions, scholarship, and creative products. (Franke, 2011, p.3)

Academic freedom also encourages students’ “independence of mind” by allowing space for them to seek information, understand concepts, and develop informed opinions (Franke, 2011 p3). The American Association of University Professors asserts:
Academic freedom, free inquiry, and freedom of expression within the academic community may be limited to no greater extent in electronic format than they are in print, save for the most unusual situation where the very nature of the medium itself might warrant unusual restrictions. (Committee A on Academic Freedom and Tenure, 2014)

By including electronic communications under the umbrella of academic expression, technology-related values are added to the cluster, including information privacy and security, and data protection.

Because the UC is a public institution, it must be transparent by disclosing certain university business records in accordance with the California Public Records Act and the Freedom of Information Act. The university does not disclose all records upon request; some include information protected by laws like the Family Educational Rights and Privacy Act (FERPA) for students, the Health Insurance Portability and Accountability Act (HIPAA) for health data, and personally identifiable information.

However, UC and UCLA have a value-based interest in not disclosing other types of records or their contents. As mentioned in the quotation above, the university fulfills its mission with a respect for academic freedom. Public-records requests can include university-held e-mails, documents, notes, and drafts. In “Principles of Scholarly Research and Public Records Act Requests,” UCLA’s Task Force on Academic Freedom acknowledges that public access is an important part of democracy, and that researchers often benefit from it. However, the authors asserted that scholarly communications should be protected “to guard the principle of academic freedom, the integrity of the research process and peer review, and the broader teaching and research mission of the university” (UCLA Senate-Administration Task Force on Academic Freedom, 2012, sec. Preamble). Scholars do not object to public access on principle, but sometimes do in practice. The Task Force distinguishes universities from other public
institutions because academic institutions produce knowledge, which clearly benefits society as a whole. Nevertheless, the document explains the accommodation:

Academia can only make these tremendous contributions to the quality of our lives if it operates according to the standards that have ensured its freedom from bias and its unwavering devotion to truth, whatever that truth may be. The threat to faculty of forced disclosure of scholarly communication through PRA/FOIA requests can damage intellectual freedom and interfere with robust scholarly communication. (UCLA Senate-Administration Task Force on Academic Freedom, 2012, sec. Conclusion)

Scholars advocate a particular scope of privacy, because an important part of academic work is the free exchange of ideas among peers. Scholars do not necessarily believe all their information should be confidential, but need an environment to voluntarily communicate information and ideas with each other, safe from prying eyes.

**Information Technology Challenges the University Mission**

IT has had an immense impact on the university and all aspects of its mission. IT opened new modes for academics to inquire, communicate, store, and share information; conduct new research; teach, present, and publish. IT has provided university administrators with tools to develop business models, approaches, and practices. However, IT has also presented some challenges to pre-digital policies and practices. Over time, the university needed new and revised policies to address those challenges in the context of values and the mission.

As the university digitized and automated its functions, concerns about information privacy and security emerged. Communication and recordkeeping practices were a large part of the advance into the digital age. By the mid-1990s, electronic records and communications clearly warranted the same consideration as their paper counterparts, and the old policies were a poor fit. As electronic communications gained traction, the threat of viruses introduced by e-mail and downloaded files plagued end users and administrators. The danger of infiltration across
networked resources established a need for comprehensive security measures. However, establishing those safeguards posed a threat to privacy.

To work effectively, security measures scan communications for threats, giving network administrators unprecedented surveillance roles and access to end users’ data and communications. Thus, early in the process, academic institutions confronted the responsibility of reconciling the antithetical nature of security and privacy. In many institutions, particularly government, the need for network security took precedence over privacy concerns, and protecting valuable equipment and data took priority. However, the UC did not overlook privacy and confidentiality concerns. The ECP and UCLA’s related policies were fundamental to UCLA’s educational mission from the outset; together they demonstrate a privacy-respectful stance while maintaining strict security standards. By invoking the mission to directly influence IT decisions, university policymakers have inextricably linked academic freedom to privacy and security.

The university had some difficulty aligning new communications and recordkeeping practices with old privacy expectations. As one interview participant explained, some end users regarded their e-mail as personal communication, an analogue to postal mail or the telephone, which they felt confident were not under surveillance by the university. Others regarded their e-mail simply as data transmitted over managed networks, with few or no privacy expectations. People’s assumptions about privacy in electronic communications depended on how they understood the data and related it to a known concept.

**University of California’s Response to the Challenges**

On November 17, 2000, UC issued the ECP (UC Office of the President, 2000). It provides principles, guidelines, and procedures related to the electronic communications services and facilities provided by the university in its mission of education, research, and public service.
It applies to all members of the university community and all forms of electronic communications. It identifies relevant state and federal law as well as intersecting university guidelines.

The ECP governs “University students, faculty, staff, and others affiliated with the university (including those in program, contract, or license relationships with the University)” (2000, sec. III.C.1.). Generally, it applies uniformly, though some differences emerged between its application to academic and nonacademic employees as a result of UC and UCLA’s strong faculty influence on governance, explored in detail later in this chapter.

To understand the significance of the ECP and its place in the university, it is important to understand how it defines a few key concepts. First, the policy is applicable only to communications technologies and not other forms of data. Communications technologies are

Any transfer of signals, writings, images, sounds, data or intelligence that is created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communications systems. (2000, sec. Appendix A)

Moreover, the policy specifically applies to electronic communications records, defined as:

[C]ontents of Electronic Communications created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several Electronic Communications Systems or Services. This definition of Electronic Communications Records applies equally to attachments to such records and transactional information associated with such records. (2000, sec. Appendix A)

Because UC is a public institution, electronic communications pertaining to university business are public records whether or not the university owns the resources used to create, transmit, display, or store them. The UC Regents own all university records, which are subject to the California Public Records Act. The ECP defines a Holder as “an Electronic Communications user who, at any given point in time, is in Possession or receipt of a particular Electronic
Communications Record.” A record is in Possession when the user has “effective control over the location of its storage or access to its content” (2000, sec. Appendix A).

Records holders are important in the ECP because the policy permits end users to use university resources (with a few restrictions) for incidental personal use, meaning that not all records generated or transmitted with university-owned equipment necessarily pertain to university business. By allowing personal use, the university hosts data unrelated to official business, but personal use introduces significant complexity to technology planning, deployment, and management. Personal communications and other unofficial business are not subject to public records requirements, so administrators (typically General Counsel) must filter them before disclosure. This step is a significant investment, but fits with the university’s commitment to its educational mission and institutional values.

The Roots of the ECP, 1960s–1990s


The ECP built on several principles and guidelines established in federal and state statues, as well as other UC policies. The roots of these policies began the late 1960s, establishing guidelines for privacy and access to information and business records. In an effort to protect the privacy interests of those individuals with personal information in records subject to disclosure requirements, the 1974 Federal Privacy Act established a “code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies” (Office of Privacy and Civil Liberties, 2015). The Act prevents the disclosure of a record about an individual from a system of records without written consent and provides individuals a means to seek access and amend their own records (Privacy Act of 1974, 1974). The Privacy Act empowers people to
control their information and designates responsibilities to record-keepers. The ability for
individuals to audit their information and ensure it must be used for the intended purpose are
guaranteed by university privacy and data-protection policy. More generally, the concept of fair
information practices pervades UC and UCLA policy and allows the university to articulate
institutional privacy values.

FERPA is also essential to privacy policy design. Passed in 1967 to protect the privacy of
students’ educational records, it grants students rights to inspect and correct their own
educational records. FERPA also prevents schools from releasing information from students’
records without written consent (with a few defined exceptions) and allows students to request
removal of their information from student directories or other public listings (FERPA, 1967).
Complying with FERPA regulations is an ongoing part of IT policy at educational institutions,
providing a baseline for all recordkeeping systems and disclosure procedures. The ECP applies
FERPA to electronic communications, forbidding disclosure of protected records.

The ECP also applies the California Public Records Act (CPRA), enacted in 1968 to
ensure government transparency. CPRA states that government records shall be disclosed to the
public, upon request, unless there is a reason not to do so. CPRA also provides a balancing test
for determining which records an agency may withhold, if it can establish that of public interest
in nondisclosure outweighs public disclosure. As a state agency, UC must align with the
disclosure requirements in this act, informing the ECP’s definition of public record and referring
to the university’s duty to determine disclosure exemptions.

In 1985, the UC issued two policies regarding privacy and access to information. “UC
Business and Finance Bulletin RMP-8, Legal Requirements on Privacy of and Access to
Information” gives comprehensive requirements for access to all types of university records. It
established “minimum requirements for developing university policies and procedures, and for
dealing with the right of public access to information and the right of privacy to individuals” (UC Office of the President, 1992 p. 2).

The UC Business and Finance bulletin RMP-7: Privacy of and Access to Information Responsibilities, established responsibilities for privacy and access to all information maintained by the university. Together, these two bulletins provided a foundation for information privacy and security policy at UC and on each campus; the EP references both as background.

In 1981, UCLA issued Policy 220: Disclosure of Information from Student Records. This policy implemented FERPA on campus, and added principles for those issues on which FERPA is silent. It named two principles to guide the campus. First,

The privacy of an individual is of great weight. The second was that the information in a student’s file should be disclosed to the student on request. It guaranteed students are informed annually of their rights, sets procedures for students to review their own records, possible access waivers, and rules about disclosure. It also defined which categories of student information are considered public, and which are considered personally identifiable information. It set procedures for students to correct records or request their information to not be publicly disclosed. (UCLA, 1981)

Electronic Mail and the ECPs Predecessors, 1990s

The ECP’s primary influence was the preceding e-mail policy, which incorporated several existing policies into a more comprehensive expression of values and principles about communication. UC issued the University of California Electronic Mail (E-mail) Policy in 1996.2 The policy’s introduction letter from UC President Atkinson stated it was produced by work by the E-mail Policy Task Force, a group represented by each campus and the Office of the President, with support from the Academic Council. At that time, a few UC campuses had e-mail policies, but none were effective systemwide. UC’s e-mail policy adapted and expanded on Berkeley’s e-mail policy, an example of the exchange of ideas between the Office of the Present

---

2 The policy and its documentation use “E-mail” and “Electronic Mail” interchangeably.
and the campuses. As stated in its introduction, UC’s e-mail policy “clarifies the applicability of existing law and University policies to electronic mail … and addresses electronic mail issues not specifically contained in existing policies” (UC Office of the President, 1996a, sec. I, see Appendix A.)

The Electronic Mail Policy identified fundamental principles about privacy, security, and the relationship between technology and UCLA community members. The policy contained several themes that are still essential, and appear in many other technology policies across UC and UCLA.

The University recognizes that principles of academic freedom, freedom of speech, and privacy of information hold important implications for electronic mail and electronic mail services. This Policy reflects these firmly held principles within the context of the University’s legal and other obligations. (1996b, sec. I., see Appendix A)

The Electronic Mail Policy established that e-mail privacy protections should be on par with those reserved for paper mail and telephone: “The University encourages the use of electronic mail and respects the privacy of users. It does not routinely inspect, monitor, or disclose electronic mail without the holder’s (as defined in Appendix A, Definitions) consent” (1996b, sec. I., see Appendix A). Some exceptions follow, including suspected violation of policy or law and time-dependent or critical operational needs. The policy states that its provisions are comparable to those that apply to conventional mail.

UC reissued the Electronic Mail Policy in 1998, with minor changes. The revision altered the introductory paragraph to include “shared governance” to the list of principles that already included academic freedom, freedom of speech, and privacy of information. The new version re-categorized the nonconsensual access exceptions, clarified their definitions, and moved them up from the appendix to the introduction. It also clarified a previously vague sentence about “Network and computer operations personnel and system administrators inadvertently see[ing]
the contents of e-mail messages” (1996b, sec. IV., see Appendix A). The new paragraph specifies that to perform their duties, those IT staff “need from time to time to observe certain transactional addressing information to ensure proper functioning of University e-mail services” (UC Office of the President, 1998b p. 8, see Appendix B).

In 1998, UC issued the *Business and Finance Bulletin IS-3, Electronic Information Security*. It established “guidelines for achieving appropriate protection of University electronic information resources (Resources) and to identify roles and responsibilities at all levels in the University of California system.” The 1998 policy requires all campuses to establish an information security program to ensure “the confidentiality, integrity, and availability of University information assets.” Each program is to assess risk, develop a security plan, and establish incident response and notification procedures, security-awareness training, and provide guidelines for third-party agreements. It also sets forth minimum requirements for network connectivity, including access control, encrypted authentication, patch management, malicious software protection, firewalls, authentications, and timeouts (UC Office of the President, 1998a). Many other IT policies at UC and UCLA reference these standards. The university updated the policy in 2003 to reflect changing technology.

Another significant driver to UC and UCLA policy was the HIPAA, passed by Congress in 1996. HIPAA set national standards and safeguards to protect individuals’ medical records and personal health information. It requires agencies and businesses collecting and storing health data to adhere to access and security regulations and breach notification guidelines. UCLA implemented these standards for its associated medical providers. HIPAA has particularly stringent privacy and security regulations, more for than for student records or many other types of institutional data. Although not all campus data are subject to its high bar, HIPAA regularly enters policy discussions about data governance, discussed later in this chapter.
Developing the ECP, 2000–2005

The ECP’s Provisions

An interviewee explained why UC had issued a policy covering only e-mail when many forms of electronic communications were emerging.

I believe there was a real intent to only look at e-mail because even in the mid 90s there was a push to address more than just e-mail, but people said, “no, lets get experience with e-mail first, and really understand what this policy is going to do and then take on a bigger chunk,” which is exactly what they did a few years later in expanding the principles.

The November 2000 ECP superseded the UC Electronic Mail Policy and the University of California Business and Finance Bulletin IS-6: *Campus Communications Guidelines*, which was alter rescinded. The policy, still in effect, does not alter the values or principles set forth in earlier policies, but applies them to a larger scope of digital communications. The ECP borrows large portions of policy language from the E-mail Policy, with minor edits. The ECP cites the same “firmly-held principles,” stating, “Principles of academic freedom and shared governance, freedom of speech, and privacy hold important implications for the use of electronic communications” (2000, sec. IV. A.). It encourages the use of electronic communications resources and makes them available to the community in support of the teaching, research, and public service mission.

After the general provisions, the ECP divides into four sections. The first is Allowable Use, which sets forth the circumstances in which the university community can and cannot use university electronic communications resources. Some usage restrictions include commercial purposes, using a false identity, or unlawful activities. It names allowable users as “University

---

3 While the discussion here is framed historically, the ECP continues to be the prevailing and effective policy for electronic of communications throughout the UC.
students, faculty, staff, and others affiliated with the university” (2000, sec. III.C.). The ECP’s Personal Use section allows members to use electronic communications resources for incidental personal use, with a few restrictions. Personal use may not interfere with the university’s operation, the user’s other obligations to the university, or burden the university with “noticeable incremental costs.” It also warns users about disclosure laws.

The California Public Records Act requires the University to disclose specified public records. In response to requests for such disclosure, it may be necessary to examine electronic communications records that users consider personal to determine whether they are public records that are subject to disclosure. (2000, sec. III.D.8.)

The next section addresses Privacy and Confidentiality, which first includes the nondisclosure statement seen before in the Electronic Mail Policy. “The University does not examine or disclose electronic communications records without the holder’s consent” (2000, sec. IV.A.). It names four exceptions, which are similar to those in the previous E-mail Policy, though developed further.

The university may examine or disclose communications records without the Holder’s consent when: (i) when required by and consistent with law; (ii) when there is substantiated reason (as defined in Appendix A, Definitions) to believe that violations of law or of University policies listed in Appendix C, Policies Relating to Access Without Consent, have taken place; (iii) when there are compelling circumstances as defined in Appendix A, Definitions; or (iv) under time-dependent, critical operational circumstances. (2000, sec. IV.B.)

Nonconsensual access must be authorized (except in the case of subpoenas or warrants) by a Vice Chancellor(s) designated by the campus in question. In all cases, the authorization is limited to the principles of “least perusal [of contents] and least action necessary” (2000, sec. IV.B.1.). Each exception includes definitions and details and states the legal circumstances that override university policy, such as subpoenas and search warrants.

The university prohibits employees from “seeking out, using, or disclosing personal information in electronic communications without authorization.” However, a provision details
that employees have responsibility for system monitoring. It explains that in the course of their duties, employees may see “transactional information or the contents of electronic communications. However, they may not search or disclose information beyond systems and operational support” (2000, sec. IV.C.1.c).

The next section addresses security, and details the university’s goal to provide “secure and reliable” electronic communications services. This section builds on the guidelines set forth in Business and Finance Bulletin IS-3, addressing security practices, system integrity, authorization, recovery, and audit practices. Communications technology experienced significant developments in the time between the implementation of UC’s Electronic Mail Policy and the ECP. The E-mail Policy warned that unless sent through an authenticated mail system, there are no guarantees that an email was sent by the purported sender. However, at the time of the policy, authentication technology was not widely or systematically in use at the university. The problem of mail interception could be solved by encryption, but “the answers to questions raised by the growing use of these technologies are not now sufficiently understood to warrant the formulation of University policy at this time” (UC Office of the President, 1998b, p. 2). Two years later, in the ECP, authentication and encryption were technological requirements.

The last section covers Retention and Disposition. It states that electronic communications records are “subject to University’s records management policies as stated in the existing University of California Records Disposition Schedules Manual,” which applies to other records as well. This section grants the responsibility of preserving electronic communications records that have been identified as “having lasting business purpose or historical value to the University” to the Record Proprietor defined in the University Records Management Program (2000, sec. VI.A.). As to backup, it specifies that UC does not maintain
centralized backups of electronic communications, and that campuses can decide if they will use backups only for system integrity, or allow retrieval requests.

**Related Policies**

After passing the ECP, a few other noteworthy developments in security policy occurred in the early 2000s. In 2003, the State of California issued SB 1386, the California Security Breach Information Act, adding new sections to the California Information Practices Act (1997; *Security Breach Information Act, 2003*). The law requires any company that stores electronic customer data to notify its California customers of a security breach to its computer system if the company knows or reasonably believes that unencrypted information about the customer has been stolen.

In 2005, UCLA issued Policy 420: Breaches of Computerized Personal Information in response to SB 1386 (UCLA, 2005). Policy 420 details the actions taken in an event of a security breach. It designates the campus officials responsible for responding to a “Suspected or actual Security Breach,” determining whether an actual breach has occurred, and whether they must notify users. The policy defines the responsibilities by campus leadership to ensure compliance in their respective organizations, and assigns the costs related to breach notifications. Policy 420 is UCLA’s most-often revised technology policy, but has typically only updated reporting and notification contacts.

**Revising the ECP 2005–2011**

The ECP is a good example of a value-based policy built to stand the test of time and has generally served the university well. Nevertheless, it needed revisions to stay relevant and serviceable. The first revision in 2005 was a response to increasing tension between the fundamental values and their implication over time. The new version addressed concerns about
access to separated staff’s communication records and security-related network-management practices. Additionally, the revision wove in UC policy changes about investigations and new records management guidelines (Craig, 2004).

The most obvious changes were additions—the revision provided more information and guidance to the User Advisories and Implementation Guidelines. It added procedures for warrants, subpoenas, and whistleblowers. It included more detail about the nonconsensual access procedure, added alternate Vice Chancellors to the list of authorized officials (in event of conflict of interest), clarified the role of Campus Counsel, and provided recommendations for separated staff. The revision added a section requiring the university to notify records holders when others accessed their communications without consent.

However, perhaps the most impactful change was also the subtlest. The original policy stated that the university would not “routinely” inspect, monitor, or disclose electronic communications records with the consent of the holder. An interviewee explained the revisions’ implications:

The 2005 revision, actually, even though it seems like it was just a few words that were changed, tweaked, as you can imagine, in the policy world, words have meaning out of proportion to what most people might think; in fact, there was a pretty subtle but significant shift in how that was worded. If I remember correctly, how that was worded in the original, pre-2005 said something to the effect of we can’t—or we don’t—routinely inspect, monitor, or disclose electronic communications records without the consent of the holder. What it says now is we don’t inspect, monitor—something like that. The words were slightly different, but the word routinely monitor went away.

An interviewee recalled one of the drivers for the change. Berkeley had implemented an intrusion detection system to detect attacks on the network in real time, rather than after the fact.

This was something that was developed at the Lawrence Berkeley Lab. … The name of the software—and I’m laughing here because I don’t understand how IT people think sometimes, even though I am one. The name of the software was “Bro.” Its like, for heaven’s sake. And we’re talking about Berkeley here! Why at Berkeley would you implement a piece of software called Bro—it’s “watching you”? 
Though the software only monitored traffic, not content, the university could no longer accurately say it was not routinely monitoring, and resulting security issues compelled a change in privacy policy. Over time, people became more accepting of automated traffic and content monitoring, but at the time it was a minor change with wide implications. In fact, people may have become more comfortable being monitored because of iterative changes like this revision.

An interviewee remembered discussions about making more substantive revisions starting around 2010, but it never happened. Each time administrators suggested the prospect of more revisions to the ECP, they received pushback from faculty groups and the Academic Senate. Faculty resisted opening the issue because they felt the outcome was uncertain. With a changing policy context and increased attention to security from recent data breaches, their fear was not unfounded. A policy overhaul could have resulted in rolled back privacy protections. Revisions experienced delays because of other policy measures as well. In June 2010, UC President Mark Yudoff charged the UC Privacy and Information Steering Committee “to perform a comprehensive review of the University’s current privacy and information security policy framework” (UC, 2013, p. 1). He also gave the committee responsibility to recommend how the university should address short- and long-term privacy issues. In light of this undertaking, university administrators decided revising communications policy before the review was finished did not make sense.

Though UC resisted a large-scale revision of the policy, it made a small change to the ECP’s implementation guidelines in 2011. Section B.6 states that the university may routinely monitor access to patient and student records, which can only be collected, stored, and accessed for business purposes. These data sources cannot be legitimately used for personal use, so no danger would ensue of infringing private personal communications. An interviewee explained that the purpose was to make clear to IT administrators that they can monitor access to certain
types of data (not necessarily the data itself) without the nonconsensual access procedure. Because law protects these records, the university must ensure that only authorized personnel can access them in the scope of their duties. According to the interviewee, the ECP revision committee attempted to include additional data sources where access could be tracked without risking privacy infringement, but struggled to define and classify them as precisely as patient and student records, so they were dropped.

**Implementing the ECP at UCLA**

Shortly before issuing the ECP issued in late 2000, UCLA released Policy 355: *UCLA E-mail Policy Guidelines*, which implemented UC’s Electronic Mail Policy. UCLA’s policy largely borrowed its provisions and policy language from UC’s version, with a few campus-specific details. Though it only intended to implement UC’s E-mail Policy, it survived UC’s expansion from electronic mail to all electronic communications a few months later. During a policy reorganization in 2004, renamed Policy 455 and with five revisions, it remained in effect until it reviewed in 2010 (UCLA, 2010).

The ECP provided implementation guidelines in Attachment 2, which left some room for campus interpretation and decision making, providing guidelines for each of four ECP sections. Several of UCLA’s so-called 400-level IT policies were written or revised to meet ECP guidelines. They, too, have undergone revisions to keep pace with law, information-security breaches, technological updates, and revisions of related policies. Occasionally, related policies did not solely address IT, but were part of broader (and often older) governance of information access, record management, risk management, and finance. UCLA policies worked in tandem with UC policy, adding campus-specific details. UCLA implemented or revised existing policy to address each guideline, as discussed in the next section, divided by the ECP’s categories: acceptable use, privacy and confidentiality, security, and retention and disposition.
Acceptable Use

UCLA issued a few policies that address acceptable use issues. UCLA’s Logon ID Information and the Bruin Online Acceptable Use Policy specify who is eligible to access university resources, and under what conditions. It covers all computing and networking services, including electronic communications. Actions such as misuse of resources, sharing passwords, or using e-mail for mass messaging can result in denial of services (UCLA, n.d.-a).

Aligned with the Implementation Guidelines, UCLA also created policy governing the appropriate use of official webpages, creation of personal webpages, and use of bulletin boards and newsgroups. UCLA Policy 411, Registration and use of UCLA Domain Names, in conjunction with UCLA Policy 110, Use of the University’s Names, Seals, and Trademarks sets standards for official webpages. UCLA Policy 311: Access to and Use of University Mailing Lists addresses mass mailing and UCLA Policy 316, BruinPost Messaging Service, provides guidelines for the appropriate use of e-mail-based services.

The ECP’s Implementation Guidelines also require campuses to respond properly to uses that violate campus policies such as copyright infringement, sexual harassment, and defamation in electronic communications. Existing UCLA Policy 464, Online Copyright Infringement Liability Limitation, addresses intellectual property concerns. Sexual harassment and defamation have their own UC and UCLA policies. UCLA’s nonconsensual access policy dictates procedures for access related to investigations and whistleblowing.

Privacy and Confidentiality

UCLA Policy 455, the local e-mail policy, originally addressed the ECP’s privacy and confidentiality guidelines. But in 2010, UCLA put the policy under review because policymakers...
determined it did not align with the ECP and needed reconsideration rather than further revision. Technically, it remains in effect but the text is no longer public; the website refers readers to the ECP document. After Policy 455 went under review, UCLA issued Policy 410: Nonconsensual Access to Electronic Communications Records to cover the policy gap left by reviewing Policy 455; it addresses the aspects of nonconsensual access that Attachment 2 assigned to campuses.

**Security**

Several UCLA policies govern information security issues, some of which are direct responses to the ECP, and others evolved separately but implicated electronic communications. UCLA Policy 401, *Minimum Security Standards for Network Devices* is one of those; it includes guidelines about software updates, authentication, unnecessary services, and physical security, all of which the ECP mentions. Another is UCLA Policy 403, *UCLA Logon ID Security Standards*, issued in 2012. It references Policy 401 and the ECP, and assigns authentication standards to users and campus service providers.

UCLA Policy 404, *Encryption of Electronically Stored Personal Information*, issued in 2010 and reissued in 2013, requires encryption of electronically stored personal information. It also designates an IT compliance coordinator and a procedure to request exceptions. The intention is to minimize the risk of information breaches. The policy states that electronically stored personal information should only be stored where necessary, and gives organization heads the authority to impose standards that are more restrictive, where applicable.

However, if other security methods fail, UCLA follows Policy 420, *Breaches of Computerized Personal Information*. Policy 420 is another policy that meets requirements set forth in the ECP, but applies to volumes of non-communications data as well. It references the California Information Practices Act, which governs state agencies that own or license computerized data including personal information. It sets requirements for those agencies to
notify California residents impacted by breaches of security of their unencrypted electronic personal information. The details about notification have changed many times since its inception, but the core intention remains.

**Retention and Disposition**

Systemwide, the UC Records Disposition Schedule set records standards, providing guidance on all records, no matter the medium (Records Management, n.d.). At UCLA, they are under the purview of the Records Management office, which handles everything from California Public Records Act requests to consulting with individual units to set up compliant systems. Typically, the same regulations apply to paper and electronic records, so implementation relies on the Records Management office.

**Values Embodied in UCLA’s Policies and Practices**

**Core Principles**

The ECP and its related policies negotiate conflicting values and responsibilities and articulates rights and responsibilities for administrators and end users. It meshes several intersecting policies and provides principles to guide IT strategy and management. To do so, it couches policy provisions with value-laden language, explicitly linking the purpose of the policy to the educational mission. First, it establishes the purpose of its resources.

The University of California encourages the use of electronic communications to share information and knowledge in support of the University’s mission of education, research, and public service and to conduct the University’s business. To this end, the University supports and provides interactive electronic communications services and facilities for telecommunications, mail, publishing, and broadcasting. (2000, sec. 1.)

Then, in the Privacy and Confidentiality section, it echoes the principles captured previously in the Electronic Mail Policy.
The University recognizes that principles of academic freedom and shared governance, freedom of speech, and privacy hold important implications for the use of electronic communications. This Policy reflects these firmly-held principles within the context of the University’s legal and other obligations. (2000, sec. IV.A.)

By weaving the institution’s values through the discussion of its responsibilities, UC and UCLA’s IT policies embed justification for each provision. If challenged, the university has a principled position to take. However, folding values into institutional responsibilities makes a governance landscape that requires careful negotiation. Academic freedom values like privacy and security can conflict with responsibilities, and in those cases, bodies make decisions by weighing the implications of each and finding an answer that does the most good (or the least damage). UCLA takes that balancing duty very seriously, and has included it in its local policies, practices, and strategy.

**Academic Freedom**

The ECP cites academic freedom as a value essential to the university mission. According to Franke, academic freedom “serves to advance the two core values of higher education.” The first is advancing knowledge through research and creativity: “Good research and creative activities need breathing space” (2011, p. 2). In this space, scholars may conduct research, publish, and create artistic works that advance knowledge in their field. In addition, they need the opportunity to evaluate other experts in their field without interference because they “may be inhibited from doing their best work if they fear offending outside forces, such as politicians or donors, or inside authorities, such as trustees and administrators” (2011, pp. 2–3). The second core value, educating students to develop their own independence of mind, allows students to experience new topics of study, ideas, approaches, and arguments without undue influence. The overarching value of academic freedom contains several specific aspects. Free speech is essential for scholars to ask questions and express ideas. Privacy and system integrity
protect those ideas until they are ready to be shared. Information sharing fosters safe spaces for scholars to communicate those ideas to other scholars, students, and the public.

As mentioned in this chapter’s introduction, IT has had an unquestionable impact on higher education’s mission. It aids scholars in every step of the academic process, from information seeking and research to teaching and publishing. However, increasing academia’s reliance on technology challenges institutions to set and adhere to standards that make the most of available resources. Higher education institutions must provide resources and meet several sets of expectations from internal and external stakeholders. This is particularly true in a state university like UCLA, which is responsible for its educational mission and its role as a government agency.

**Privacy and Confidentiality**

**Access without consent at UCLA.** The nonconsensual access provisions in the ECP and UCLA’s Policy 410 reflect a desire to protect individual’s privacy without sacrificing other institutional needs. The process for requesting access to communications without consent is deliberately arduous. It begins with the requestor submitting a form detailing the reason for the request and the scope of the data included. Before approving the request, the designated authorizing agent (a Vice Chancellor) confers with Campus Counsel. The requestor must specify which of the four exceptions apply, according to ECPs parameters. For instance, a compelling circumstance is one in which “failure to act might result in significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of University policies listed in Appendix C, Policies Relating to Access Without Consent.” But other exceptions are less precise: a “time-dependent, critical operational circumstance” is one in which “failure to act could seriously hamper the ability of the University to function administratively or to meet its teaching obligations, but excluding circumstances pertaining to
personal or professional activities, or to faculty research or matters of shared governance” (2000, sec. IV.B.). Nevertheless, no matter how detailed the definition, a Vice Chancellor has a degree of discretion.

UCLA included additional privacy protections in its local nonconsensual access Policy 410. Some other UC campuses designated the Chief Information Officer to authorize access requests, but UCLA opted to distribute authorization decisions. At UCLA, four Vice Chancellors field requests from their respective deans, department heads, or unit heads. Faculty, students, staff employees, and medical staff each have a designated Vice Chancellor. Campus Human Resources provides consultation for staff employees. An interviewee shared that policymakers felt a Vice Chancellor would be most informed about his or her area, and therefore able to grasp the context of a request and its possible implications. Each UC campus is also responsible for conferring with their Academic Senate to establish procedures concerning faculty holders. UCLA opted to consult with the chair of the Academic Senate and receive written advice and a recommendation for each request. Each of these individuals has an opportunity to opine before recommending or not recommending access, or ask for clarification or a narrower selection of records. The idea is that several reviewers will apply a balancing test to the request, weighing privacy interests against the significance of circumstances. However, the assigned Vice Chancellor makes the ultimate decision, allowing a degree of discretion, meaning that exceptions may vary based on scope or recipient. The Vice Chancellor may choose to override the recommendations in the final decision, though interviewees suggested this was extremely rare. Because UCLA chose to have more than one authorizing official, it relies on those employees holding the same values and policy interpretations, to the extent possible.

**UCLA’s interpretation of records holders.** The ECP’s Implementation Guidelines give campuses the responsibility of implementing procedures for separated employees. After staff
employees leave the university, the privacy policy no longer protects them; thus, the university may access their communications without consent or use of the nonconsensual access procedure. In 2012, UC’s Office of General Counsel affirmed this interpretation and communicated it with Campus Counsel offices. General Counsel’s interpretation hinges on the definition of an electronic record holder. The ECP defines a “Holder” of an electronic record as a “user who, at a given point in time, is in possession” of the record. The ECP further defines possession of a record as when an “individual has effective control over the location of its storage or access to its content.”

When staff leave the university and cannot access (or should not be able to access) their communication records, they are no longer in possession of the record, thus are no longer the holder. No individual any longer has possession of the records, so institutional access does not require permission. However, UCLA practice does not consistently align with this interpretation; decisions about how to handle saved communications from separated employees varies among campus units; some departments regularly follow UCLA Policy 410’s nonconsensual access process for all separated employees. Confusion about the issue persisted; in May, 2014 UCLA’s IT planning committees received General Counsel’s interpretation, surprising support staff committee members unaware that the policy treated staff members differently. Some committee members believed the interpretation contradicted UCLA’s position on privacy in general, and voiced concern.

When members of UCLA’s Campus Computing Cooperative asked for clarification about this position, the Chief Privacy Officer (CPO) confirmed General Counsel’s interpretation and

5 This pertains only to staff members; faculty retain privacy protections even after they are no longer employed by the university.

6 The Common Systems Group and the Campus Computing Cooperative were two committees mentioned by interview participants, which was supported by meeting documents.
noted it was consistent with wording of the ECP. However, he also stressed that “just because we can do something doesn’t mean we should.” The CPO noted, “it’s important to consider that UC has had a long history of tilting in favor of protecting individual privacy,” a notion confirmed by systemwide privacy-related efforts at the time, discussed further in Chapter 5. The CPO did not go so far as to recommend unnecessary use of the nonconsensual procedure, but instead encouraged departments who were considering the stricter interpretation to notify incoming and outgoing employees about their privacy protections (K. Wada, personal communication, April 24, 2012).

By 2014, the campus recognized a need to formalize policy and procedures to address the issue and was still in the process at the time of this project. Until the policy is complete, policymakers have undertaken the interim task of providing local human-resources units with the information they need to properly inform new and separating employees about their privacy expectations. Educational outreach is an important part of policy implementation regardless of the final decision about employees’ status as records holders. As the campus expands its technology infrastructure to include off-site cloud services, increased awareness about information access and ownership will be essential to ensure that the ECP and other data protection policies serve the university and its members.

**Security**

UCLA’s IT services aim to strike a balance between protecting and sharing information; enabling the proper flow is key to academic freedom. ECP protections against nonconsensual access and disclosure are quite important. However, those protections only protect scholars from internal surveillance and external records requests. The other part of protecting private communications is to keep them safe from bad actors, internally or externally. This aspect
requires robust information security protocols. Yet, university networks should not be so impenetrable that they impede information sharing and collaboration.

UCLA has a strict interpretation of network monitoring practices regulated by the ECP in comparison with other UC campuses. UCLA differentiates between automated processes and human processing: the former is more acceptable than the latter, though they involve variation and constant negotiation. For instance, in principle, the Chief Information Security Officer (CISCO) supports automatic monitoring of e-mail headers to protect against viruses and piracy attempts, but does not monitor message content. Many other campuses use software to scan entire servers for personal identifying information such as security numbers and drivers’ licenses. However, the CISCO’s position is that those activities violate the policy, and decided against adopting it. However, the campus did adopt an automated spam-detection system characterized by the CISCO as “dancing on the edge of the ECP” because it scans content and quarantines questionable mail. A user can disable content scanning at the account level, but must know it is an option and how to change application preferences.

In 2006, UCLA security technicians discovered a nearly year-long data breach at UCLA that exposed personal information of approximately 800,000 students, faculty, staff, and some applications and some applicants and parents (Lin, 2006). After analyzing the breach, the campus activated a system to map Internet protocol (IP) addresses to end users, two data points that are not considered sensitive on their own, but in combination can track end users’ physical locations. This significant decision marked a point at which IT departments had to weigh the possible dangers of tracking authorized usage with the ability to thwart confirmed methods for unauthorized access. The breach was discovered when security staff noticed compromised user credentials, and that unauthorized people were using them to access the system from several different physical locations, typically foreign countries. While successful, the problem with this
method was that administrators were able to see end users’ locations and other login data, a type of surveillance that arguably subverts the intentions of the ECPs anti-monitoring mandate. The university addressed this problem by deploying automated software that scans network traffic and alerts the end user when it detects suspicious activity. The e-mailed alert directs the user to verify legitimate activity or change their password. Many networks on campus employ methods like these, deeming automated monitoring an appropriate balance between privacy and security interests.

Other changes in security-monitoring practices have come about through broader changes in infrastructure and governance. As a campus referred to by one interviewee as “dysfunctionally distributed,” UCLA has struggled to maintain security standards and practices across its many networks. The campus’ decentralized IT has shown strengths and weaknesses; local units have been able to identify and serve the needs of their groups, but even with collaborative efforts have lacked cohesive security measures. Greater centralization of IT administration in recent years has helped standardize information security. This advantages the fight against data breaches, but bringing larger portions of network traffic under fewer system administrators highlights the need for constant privacy/security balancing.

Balancing Values in UCLA’s Information Technology Policy

UC has addressed information privacy issues in a multitude of ways, one of which was through the 2010 UC Privacy and Information Security Initiative, which reviewed the entire privacy and information security framework to make recommendations. As mentioned in an earlier section, this initiative contributed to a delay in further ECP revisions, but served privacy values in a more comprehensive way than was possible through a single communications policy. The initiative concluded with a final report recommending a Privacy Balancing Process, 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 process “considers the parties’ interests, benefits, burdens, and consequences associated with the proposed action.” It gives examples of factors to consider when applying the test, such as risks and benefits to each party, alternative less-intrusive approaches, and time or monetary costs (UC Privacy and Information Security Initiative, 2011, p. 18). Interviewees recalled applying the balancing test in several different types of circumstances; the most common were in making decisions about how to meet public-records requests, and how to maintain privacy values in the face of increasing security threats.

**Balancing Privacy, Transparency, and Efficiency**

Academic freedom values can sometimes conflict with a state institution’s transparency responsibilities. As a public institution, UCLA’s business records are subject to disclosure, which can include academic work and scholarly communications. Whether transparency is an institutional value or duty depends on perspective. Researchers seeking public information value transparency, but fear the chilling effect of overreach.

Robust, frank, honest exchange depends on the maximum protection of the informal and everyday work, personal e-mail, drafts, and records related to research and teaching. It is essential that regular and frequent communications among faculty within UCLA and with colleagues in other institutions remain within faculty control. (UCLA Senate-Administration Task Force on Academic Freedom, 2012, sec. Preamble)

Faculty at UCLA have concerns that fear of disclosure, particularly before research is published or taught, will steer scholarship away from controversial issues. For example, private industries may use public-records requests to mine valuable data from unpublished research, hampering competition. Open record laws have a profound potential impact on scholarship, but other disclosure requirements come from journals with open access policies and funding-agency requirements. Reconciling these values and responsibilities can be complex, necessitating clear
policy and consistent implementation. The ECP’s incidental personal use clause complicates transparency responsibilities, because personal communications are not subject to disclosure. In the event of a records request, a university employee will likely need to search all communications in that user’s university-owned account to determine which are business records and which are not.

As mentioned earlier in this chapter, the ECP has undergone relatively few changes since its inception; its core values of privacy and security as fundamental aspects of academic freedom remain. What has changed is the context of the ECP, and the way the university negotiates conflicting values and responsibilities. One of those changes is a dramatic increase in public records requests received by UCLA over the past 5 to 10 years. UCLA’s Task Force on Academic Freedom explained the problem in their 2012 statement:

[T]hese requests have increasingly been used for political purposes or to intimidate faculty working on controversial issues. These onerous, politically motivated, or frivolous requests may inhibit the very communications that nourish excellence in research and teaching, threatening the long-established principles of scholarly research. (UCLA Senate-Administration Task Force on Academic Freedom, 2012, sec. Preamble)

The proliferation of open records requests has influenced the way the ECP impacts campus business. Public records laws have not changed, but the standard for privacy protection has been lowered as a matter of course. More requests result in a higher volume of information for the university to search, assess, and disclose. Administrators are challenged to effectively teach employees about the reach of the law and how it can affect them. An interviewee remarked that those who receive requests are often “unpleasantly surprised” because they were unaware of what can be exposed.

To accommodate the influx of requests, UCLA formed a Records Management and Information Practices Office. The requests received are wide-ranging; many fall under the spirit of the law, but some have questionable goals. Most problematic for the university are requests
that include those seeking unpublished research for market competition, those trying to intimidate academics with controversial topics, and those that ask for such a large volume of information that burdens the individual involved, decreasing their productivity. Public universities also hold concerns that their disclosure requirements make them less competitive than their peers at private institutions that have a higher level of privacy.

To mitigate those concerns and avoid disclosing information outside the scope of the law or the request, the university decides which information to disclose and which to protect to maintain academic freedom and personal privacy. The law has some clear disclosure guidelines allowing the university to redact records containing personally identifying information or health data. But the responsibility to protect scholarship rests on the university, meaning that, by choice, it can withhold scholarly communications that fall under the academic freedom category.

Balancing Privacy and Security

The IT governance structure at UCLA encourages a balance of privacy and security values, as well as the duties associated with them. Several interview participants in this project recognized that administrators, IT staff, and faculty have a dialectical relationship with the written policies, informing and being informed by them. Ongoing collaboration across units in UCLA’s decentralized environment is a point of pride among IT employees who recognize that their roles and relationships are different from those in other educational institutions, but that they are appropriate for UCLA’s institutional culture. UCLA’s CPO position, the first of its kind in the UC system, is one very visible example of this value. The CPO makes strategic and operational decisions related to information privacy. It is rare for a higher education institution to have such a dedicated position, and even rarer for it to be as privileged as it is. At UCLA, the CPO and CISCO hold similar positions in the organizational structure, with the CPO addressing
academic viewpoints and the CISCO addressing administrative viewpoints. This dichotomy reflects their duties and overall purpose, and highlights the difference between the two interests. Typically, if a university has a CPO, they are a part of a compliance office and have a primarily administrative function. At UCLA, the CPO is concerned with compliance, but approaches privacy issues in a much broader context of institutional values.

The CPO and CISCO have responsibilities that often conflict, but have made a continual effort to cooperate. Cooperation of this nature has been problematic at a few other UC campuses; an interviewee told the story of an incoming privacy-oriented CISCO at another university who clashed with network system administrators, resulting in a breakdown of communication and trust. By contrast, IT employees from different units at UCLA work to accommodate each other’s responsibilities, and are largely satisfied with the results. Interviewees often discussed the importance of collaboration in UCLA’s institutional culture, illustrated in the effort to bridge the academic/administrative division in IT units, in ideals and practices. A security technician remarked,

I work with the system. But you can’t really fight it. If you don’t have some sense of the academics; it would be a disaster. There have been people at other campuses who come and they want to make all sorts of changes and they’re gone in a year. They feel like they can’t get anything done.

By nature, collaboration in a decentralized institution is difficult, and not everyone is satisfied with IT-related decisions (or find them difficult to make in the first place). Nevertheless, interviewees understood the necessary balance between privacy and security, why each is critical for the campus, and had ideas about how to balance them. They did not always agree that the campus had achieved that balance, but regardless of their designation as academic or

---

7 The CPO is part of the OIT, which has primary responsibility for supporting academic and research functions, led by the Vice Provost for Information Technology. The CISCO is part of the Information Technology Services office, headed by the Associate Vice Chancellor, which supports primarily administrative functions, though significant crossover ensues into instruction and research.
administrative employees, interviewees were well aware of the needs and goals of each side. They recognized collaboration and cooperation as a necessary part of UCLA culture.

In this case, the CPO and the CISCO are particularly good representatives of their roles, which was clear in interviews as well as in my experience working with them. The CPO tends to take an academic approach to issues by “looking for the overarching principles and [breaking] everything down in a very kind of methodical but high-level approach,” as characterized by an interviewee. By contrast, the CISCO came from a government background where no privacy expectations existed in information and communications; thus, the CISCO focuses on practical measures. Both are committed to the same values, though some tension arises between their responsibilities. One recalled “many heated discussions” about the difficulty of providing adequate security under ECP constrictions. Employees like these are a reminder that human resources are an often-overlooked but vital part of the IT infrastructure that contributes to policy context.

**Advantages and Drawbacks of the Balancing Test**

Balancing tests have advantages and disadvantages for institutional decisions. They help campuses look closely at their own records and make policy-grounded decisions. However, decisions are subject to the discretion of a few people who must weigh many factors at once, negotiating institutional values, the university mission, and multiple responsibilities. While explaining the process, an interviewee referenced the well-known Supreme Court Justice Stewart’s comment on pornography—that he could not succeed in defining it but that he knew it when he saw it (*Jacobellis v Ohio*, 1964). The comparison gives insight into the inherent ambiguity and need for those applying the test to have intuition based on experience. Because the policy avoids prescribing precisely how to apply the test, the result depends on the adjudicator’s
perspective on privacy and what is best for the university, along with whether he or she follows precedent.

Even if UCLA happens to have the best possible adjudicators at any given moment, if they leave the university, they take with them institutional knowledge and their personal morality; a replacement may not follow precedents. One interviewee saw that eventuality as a weakness in the ECP and wants clearer guidelines so the test can survive beyond any individuals responsible for employing it. Another administrative interviewee understood the argument for clearer guidelines so the policy would be less “subject to the sort of whims or personality of the people involved.” But even with more specificity, balancing tests are inherently subjective. Two interviewees proposed different balancing approaches. The first places the greatest importance on objectivity and consistency, advocating for more specific guidelines. The second proposed the opposite approach, arguing that the policy should be less prescriptive, keeping the policy flexible enough to be relevant over time. In either case, capturing an effectual balancing test in writing is a difficult task.

**Potential Future Challenges to UCLA’s Approach**

Further ECP revisions may be necessary; some interviewees had a sense that the policy has not kept pace as well as it could have. One remarked, “it’s not that the principles are wrong, but how they might be expressed may need to change.” Another interviewee was critical of the policy’s prescriptive nature, particularly in the nonconsensual access procedures, for instance. The interviewee pointed out that the policy not only states its privacy intentions but also instructs campuses about how to implement them. Thus, it may not be flexible enough to address issues that were not even a possibility when the policy was written. Rather than attempting to write policy to cover every possible future circumstance, the principles and balancing test should be strong enough to provide guidance in areas the ECP does not address.
As an example, some policy fundamental assumptions about technology are out of date. The policy language refers to protecting assets, the machines themselves. Data protection was less of a focus in the late 1990s than it is now. Current security concerns expand far beyond computers and devices (though the need for their protection has not lessened) and now include data transmitted and stored in many different locations. The types of communications records have expanded as well. Although the ECP governs all communications records, it still primarily pertains to e-mail and may not be adequate to cover other types of digital communication essential to academic freedom. For the ECP to maintain continued longevity, it will be important for policymakers to avoid specific technology and focus instead on strengthening the mechanisms that evaluate emerging technology in context of institutional values.

**Maintaining a Principled Position**

With the ECP and UCLA’s local implementation, the university takes a particular position by committing to academic freedom values, and stating that they can not meet their academic mission without them. By taking a hard policy line and building an institutional culture around it, UCLA sets itself apart from other higher education institutions. Interviewees responsible for information security on campus emphasized how provisions in the ECP and UCLA’s approaches perplex other IT professionals. They experienced this perplexity when they communicated with their peers at other institutions. Not simply do other universities favor network security over privacy (though they often do), but they can deploy software and monitoring techniques that they consider industry standards, whereas UCLA cannot. UCLA’s CISCO encountered a disconnection even from other UC campuses because UCLA has a stricter interpretation of the anti-monitoring ECP mandate. An interviewee confirmed this view, telling a story from a security conference panel:
[W]e were talking about what we could and couldn’t do in terms of security and I said, “We have this policy that prevents us from monitoring what people are doing generally, unless there’s a legal reason or something like that, and you might think we’re insane but its very privacy respectful.” And the person sitting next to me on the panel stood up and said: “Yes, I’m one of those people; I think you are insane. It’s ridiculous, how could you have such a ridiculously restrictive policy?” It was a security officer; he felt it was constraining.

Another IT employee recalled IT colleagues expressed similar sentiments when they met with peers at other universities to discuss “bring your own device” (BYOD) issues. UCLA allows faculty, students, and staff to use personal laptop computers and mobile devices to connect to university networks and access business records or other sensitive information. BYOD poses a number of security risks, and initially system administrators at UCLA (as well as other institutions and businesses) resisted supporting them. But the proliferation of mobile devices combined with rising demand eventually brought the issue to the forefront, compelling the university to develop a strategy for managing them. In this process, UCLA’s system administrators expressed frustration that they could not use the tools and methods common to other institutions because they conflicted with privacy policies.

BYOD presented a number of privacy and security issues, and was a slow-moving process, slower than the rapidly increasing use of personal devices on campus. By the time governance committees considered the proposed strategy, administrators had to admit that “the horse had left the barn.” Administrators made decisions reactively, rather than proactively. Policymakers were baffled by the prospect of decreasing end users’ convenience or sacrificing security standards. Rolling out a BYOD strategy was much easier at other universities without the ECP’s monitoring restrictions. When relaying the difficulty of addressing issues like BYOD, a system administrator explained that fellow IT peers were incredulous that UCLA cannot employ common management methods.
And I’ll look at them and say, “My policy; I can’t do that.” And I start explaining the ECP, and it’s like, “Naw … that can’t be right.” And I’ll say, “No that is UCLA policy.”

The ECP’s focus on protecting academic freedom and its associated values affects IT policy in many ways, driving decision makers to craft unique approaches and solutions to even the most common IT issues. Although interviewees expressed frustration at the layers of difficulty that policy adds to their duties, none gave the impression that too many constrictions left them unable to provide quality services. Employees often felt confusion and resistance at the beginning of their tenure at UCLA, particularly if they came from other universities, but after more time in the culture, they contribute to a policy context that adeptly fulfills university values with appropriate and often creative methods.

**Cloud Computing and External Vendors**

The ECP only applies to electronic communications, but many UCLA employees maintain the same expectation of privacy for their other data, whether or not policy secures it. As new technologies such as cloud computing have exploded in popularity, UCLA has struggled to educate its community about their privacy rights and how and where they apply. Most employees, particularly faculty, are aware that the university does not monitor or disclose their communications without consent. However, they are less sure about the reach of the policy or which of the many software services and platforms comply with it. The ECP states, “University contracts with outside vendors for electronic communications services shall explicitly reflect and be consistent with this Policy and other University policies related to privacy” (2000, sec. IV.A.). But the issue becomes more complicated with third-party services that blend communications with other data.

The best example of this blending is commercial Google Mail and Apps. Google provides a no-cost suite of Web services under one user account, including e-mail, social media,
YouTube, document storage and sharing, and videoconferencing. Continual integration of Google’s acquisitions promises convenience and added features for end users. However, it also funnels a vast amount of personal and business data and metadata into one platform, administered by an external vendor. Because UCLA does not block Web content on its network or university-owned computers, end users may access and use third-party services. The problem is that university records should not be stored on non-UCLA managed servers. The university must be able to access files subject to disclosure, and ensure the ability to meet legal and policy requirements.

The fundamental problem with third-party commercial services is that the companies’ terms of service agreements govern them. This is a problem for university business for two reasons. One is that employees do not have the authority to sign agreements (such as a click-through consent on a terms-of-service statement) on the university’s behalf. The second problem concerns the conditions in those terms. The service provider writes them to serve the company’s interests, which often conflict with university privacy and security requirements. For example, most technology services sustain active monitoring processes for protection and content assessment for targeted advertising. That type of monitoring is a direct violation of the ECP. Additionally, many research projects have grant or Institutional Review Board (IRB) restrictions that do not align with vendors’ data management practices.

However, the scale and availability of free commercial platforms means that end users are likely to adopt them personally, and then want to use them for research or instruction. Many do not know or do not care that using these services is a violation of the ECP. IT administrators are sympathetic to their desire for familiar, convenient, and feature-rich services, but struggle to give users the capabilities they want in ways that do not violate policy. This discrepancy is a point of contention on campus; people want to use the same services they use for non-university
business, not understanding how or why those services are inappropriate for official use.

Additional confusion accrues because the university encourages employees to use third-party services for personal communications, voluntarily separating them from business records. This good advice ensures personal communications are not subject to review in the event of a public-records request. However, following the advice requires end users to maintain separate accounts and credentials.

Instead of outright banning popular third-party services for official business, the university works with popular vendors to create UCLA or UC-specific agreements that offer services without violating policy. UCLA has had varied success with this approach. Easily the most significant was with Google because it resulted in a lengthy negotiation between multiple stakeholders. The outcome set the standard for future discussion about outsourcing local technology services to third parties. Since the 1990s, UCLA had hosted its own campus e-mail service, but by 2008, the infrastructure was nearing its end-of-life. At the same time, Google captured the attention of some administrators by offering host university e-mail accounts for no cost. At first glance, many other universities had adopted an obvious cost-saving solution. But privacy and security officers noted substantial problems with the idea and began warning technology planning committees, frustrated that they seemed oblivious to the implications:

I was going, “Time out guys—you’re not thinking about this.” I went to the [Information Technology Planning Board] and eventually laid the whole thing out. It was before they called it cloud data. And I was like, “You are giving up a tremendous amount of things—that could be looked at as a violation of the ECP, in fact.”

One of the reasons Google can afford to offer its clients free services is that it scans the contents of e-mails sent over its servers to present account holders with targeted advertising. That factor alone is enough of an ECP violation to exclude Gmail as an option. But several other objections emerged—all with merit—though they complicated the continued discussion.
In response to this and several other cloud computing proposals, the UC’s Information Technology Leadership Counsel created the Cloud Computing Task Force in May 2009 to assess cloud computing and its applicability in the UC system. The Task Force’s report recognized the vast potential to advance the institutional mission with outsourced IT services, but named numerous concerns beyond scanning e-mails for marketing purposes. They argued,

The lack of a well-understood and adopted policy and legal framework for outsourcing IT services for UC is the single largest barrier to the adoption of cloud-based services. It is also likely to lead to inappropriate use of cloud-based services in the future, putting the University at risk of privacy breaches and service losses. (Cloud Computing Task Force, 2010, p. 8)

The considerations outlined in the report became the backbone for current software-as-a-service vendor negotiations. When the university gives a vendor control of its data, it is subject to the third party’s business plan, which is not subject to the ECP, values, or mission. A privacy issue arises because cloud services may store data in locations outside the state or country, where local privacy laws may differ, allowing disclosure that would be disallowed by university policy or U.S. law. Another problem arises if the vendor sells or goes out of business; their practices regarding transfer or destruction of data may not correlate with university polices. Several issues also arise around questions of access, ownership, and responsibility. As a data owner, the university has legal obligations to protect it, and is liable if the vendor does not meet the same standards. Defining data owners and data holders and assigning rights and responsibilities to each is a complex issue that needs thorough assessment before outsourcing.

Eventually, UCLA successfully negotiated a contract with Google that outsourced university e-mail accounts and gave end users access to most of the bundled Google applications available to commercial accounts. The contract precluded Google’s typical content monitoring practices to meet ECP requirements. However, other vendors like the document storage service Dropbox, refused to make agreements. In an attempt to provide an alternative, the university
contracted with Box, a different vendor with a similar service. UCLA signed a contract with Box and began a pilot deployment. But years passed during negotiation and during that time, end users adopted the more popular Dropbox, whether or not they understood the policy conflict. The university attempted to communicate with community members about this, sending e-mails and encouraging technology-support units on campus to spread the word and advise users accordingly. Outreach efforts did not have the desired widespread effect. By the time UCLA’s enterprise version of Box was available, those who had adopted Dropbox in the meantime were disinclined to switch services.

The university faced a similar struggle when deploying the licensed version of Google’s services. Aside from common data and account-migration issues, UCLA faced an end user base with wildly different opinions about Google and its business practices. In the intervening years, many faculty and staff became particularly attuned to privacy issues. They distrusted Google’s monitoring practices and its ability to develop algorithms that make large sets of metadata meaningful. Others remained unaware or unconcerned about Google’s reach into their online behaviors, but did not grasp that the UCLA and commercial services were different for policy reasons. The community continues to experience a mix of information and opinions with varying degrees of accuracy and legitimacy which unsurprising for such a large institution, but difficult to manage.

The struggle to encourage end users to adopt university-approved services is a familiar topic among support technicians. They reported a few common factors in the reluctance to switch. Some end users incorrectly assumed that their data did not fall under the classification of university business or simply were not aware of IT policy. Many objected to the time and effort it takes to adopt an unfamiliar service, even if it has the same functionality. Also, end users want the same services their colleagues in other institutions use, such as Dropbox, which has a much
wider customer base than its competitor Box. Switching services requires end users to lose some short-term productivity; even with a compelling privacy argument, it is difficult to convince them to make the initial commitment.

Although users’ reluctance is an issue, they are not solely at fault. The university provided little education and outreach on this topic, particularly in the beginning. In the case of Dropbox, IT staff circulated a few e-mails explaining that it was prohibited for university business, but the e-mails were not particularly compelling. Some solid efforts ensued to remedy the information gap and apathy. The OIT hosted events to explain the details and implications of cloud service usage. However, the lag between the university telling people they should not use a popular service and providing a useful alternative was detrimental. The UCLA Privacy Statement (discussed further in Chapter 3) includes a section with practical advice about dividing personal and university communications among different accounts, policy readership was too low to make a significant impact. Decentralization and the lack of consistent outreach put the message at a disadvantage. Decentralized IT administrators can effectively spread a message on the local level, particularly where IT staff has a relationship with the people they support. But an organized effort at the top must set it in motion and support it to reach the lower branches.

**Conclusion**

Institutional values play a critical role in the UCLA’s IT policy. They are not entirely static; their significance and influence can fluctuate over time as the institution experiences shifting duties and responsibilities. A commitment to academic freedom requires UCLA to resist characterizing privacy and security values as oppositional forces, conceptualizing them instead as necessary components of the same system. As demonstrated in this chapter and the next, UCLA’s IT governance establishes privacy and security standards as a baseline when making IT policy decisions. For instance, vendor contracts, like those in the previous section, have evolved
to add privacy and security considerations to other technical criteria typically the focus of system administrators.

To trust that UCLA nurtures academic freedom, scholars want evidence of the university resisting intrusion into online behavior while maintaining access to new technologies. But the process to infuse value-based privacy and security standards into vendor contracts is complicated. Managing the interests of the user-base, IT support structures, and administrative policy is an intricate endeavor that requires more than policy. It requires an IT governance structure composed of distributed interests, as analyzed in the next case study. In both of the remaining studies, it is important to note that UCLA’s IT policy often diverges from that of other institutions, and when it does so, it is typically a result of the university fulfilling an institutional value or its educational mission.
CHAPTER 3

UCLA’S GOVERNANCE STRUCTURE AT WORK

UCLA ADVISORY BOARD ON PRIVACY AND DATA PROTECTION

Overview

In UCLA’s IT policy development, the institutional values discussed in Chapter 2 have a relationship with its IT governance. This chapter explores governance structures and practices at UCLA, and their links to values, in an examination of UCLA’s Advisory Board on Privacy and Data Protection, a body that, in many ways, typifies the UCLA approach to IT policy. The Privacy Board’s role in the university’s governance structure, and its function as a critical part of IT governance processes provide a prime example of how the university’s policy context develops.

UCLA’s Privacy Board is a significant example of how institutional values do not only inform governance, but also drive it. Values particularly influence privacy as it relates to the pursuit of academic freedom, but also freedom of speech, information sharing, IT systems integrity, and shared governance. The Board is UCLA’s answer to the balancing work delegated to each campus by the ECP. In understanding why this board exists, how it functions, and the particular challenges it has faced over time, the ECP’s values are clearly applied through shared governance and put into practice in a unique way.

This chapter introduces the Privacy Board and uses the voices of participants who recalled its birth and growth over time. It begins with an explanation of the Board’s operations and its role in broader governance structures at UCLA and the UC. Drawing together interviews and documentation (including charters, publications, letters, e-mails, agendas, and meeting notes), the chapter explores the bond between UCLA’s values and policy implementation. In the
course of reviewing and analyzing the Board’s history, the chapter highlights key issues the Board addressed, such as digital recordkeeping, social media, faculty dossiers, and illegal file-sharing. The chapter proceeds with an evaluation of the Board’s Statement on Privacy and Data Protection (hereafter referred to as the “Privacy Statement,” as it is commonly known on campus) and UCLA’s influential role in a similar statement for the UC system. The chapter closes by discussing challenges likely to confront the Board in the future, using the Data Governance Task Force as an example. I argue that the Task Force is an example of the Privacy Board’s continued influence on UCLA’s IT governance structures.

**Background**

As introduced in Chapter 1, institutional governance refers to the organization’s governing actions, which include formal policy, decision-making bodies, and formal and informal practices. Mark Bevir argued that increasingly, in government and organizations, governance refers to “the rise of new processes of governing that are hybrid and multi-jurisdictional with plural stakeholders working together in networks” (2012, p. 5). This was an apt description of IT governance’s complexity at UCLA, which is governed by UC but is also responsible for serving multiple interests through its own governance structures and decision making.

UCLA and UC operate under a shared-governance model that includes academic personnel in decision making involving academic endeavors. In this model, the university’s administration and faculty have responsibility for different parts of the institutional mission, and together share in the management and operation of the university. By allowing academic employees to be the primary decision makers about curriculum, teaching, and research, the university can ensure an appropriate focus on the educational mission. Although it is more involved in U.S. primary and secondary education than higher education, the American
Federation of Teachers, for example, argued that participating faculty can offer resistance to the belief that “higher education is an industry like any other and should be run on a ‘business model’ of central command and control” (2002, para. 3). The Federation sees the business model as a threat to academic freedom and the educational mission, pointing to increasingly common practices like reassigning teaching duties to lower-paid non-tenure-track faculty, reducing liberal arts offerings, outsourcing course design, and appropriating instructors’ intellectual property for courseware. By sharing institutional responsibilities, the model aims for balanced representation from academic and administrative employees.

In UC and UCLA, tenured and tenure-track faculty comprise the Academic Senate. Senate members elect members of a legislative bodies at each campus, as well as the statewide level, known as Legislative Assemblies, to represent their interests and those of their academic units and programs. The Legislative Assemblies and their standing committees, as well as ad hoc committees and task forces, perform the Senate’s routine work. At the broadest level, the Senate oversees admissions and degree-completion criteria, supervises curricular and academic programs, sets and applies standards for faculty hiring and advancement, and advocates for faculty interests. UCLA splits governance responsibilities between the Senate, focusing on teaching, research/scholarship, and service; and with university administration, focusing on facilitative infrastructure and operations. For instance, Senate members have primary oversight over hiring, evaluating, and promoting colleagues and instructional content. The administration, in contrast, is responsible for campus resources and their management (Karagozian, 2010).

Thus, UC and UCLA have relatively powerful faculty representation, which exists in a productive tension with university administration. This tension helps ensure the administration takes the faculty’s academic interests seriously, even when the two groups’ interests or perspectives diverge or conflict. In many other institutions of higher education, particularly
private institutions, faculty must often cede nearly all academic decision-making power to administrators, whose staff may adopt market-style organizational “business models” that mimic those in private-sector industries or commerce. A faculty that reserves primary control over courses, teaching, and advancement, especially in institutions facing budgetary strains, is becoming increasingly rare in other U.S. universities.

However, the shared-governance model is an essential part of UCLA’s policy context. As the three cases in this study suggest, each time policy bodies depart from policy trends that are more typical in other universities, the difference often traces back to strong faculty influence. At UCLA, academic values are infused into each step of the decision-making process from the stage of identifying issues that need attention through to policy implementation. Faculty members directly engage in each policymaking stage, often by participating in joint academic/administrative governance bodies, such as the one discussed here.

**UCLA’s Shared IT Governance**

University administration and the Academic Senate share governance duties at the highest level, but the division of labor trickles down to IT policymaking bodies as well. As mentioned in Chapter 1, two of the three technology governance committees on campus have joint membership—the ITPB and the Committee on Information Technology Infrastructure.

UCLA’s ITPB, responsible for the Privacy Board’s formation, is a joint Administration–Senate committee that acts as the primary governance and oversight body for IT on campus. UCLA’s administration formed the ITPB in 2000 as the successor to the Academic Information Technology Board in response to “the increasingly interrelated realms of academic and administrative computing, and centralized versus decentralized deployment of resources.” ITPB membership comprises a faculty chair along with “current senior academic administrators, administrators, and additional faculty, with the faculty predominant.” Its responsibilities include
a mix of visionary, strategic, policy, and budget matters (“Charter for the Information Technology Planning Board,” 2000, sec. Chair, Membership, and Duration, para. 3).

A few points from ITPB’s charter indicate the environment in which the Privacy Board was introduced. Shared governance themes and language exist throughout the ITPB charter:

The Board must ensure that its actions are consistent with academic-based decision-making and joint governance, as these concepts have evolved at UCLA. In this regard, the Board will create an environment conducive to broad-based consultation among UCLA’s faculty, administrative leadership, Academic Senate leadership, students, and staff. (“Charter for the Information Technology Planning Board,” 2000, sec. Responsibilities, para. 3)

The same themes and joint membership model influence other governance committees on campus, like the Privacy Board analyzed in this chapter, the Committee on Information Technology Infrastructure, and the Data Governance Task Force (discussed below).

In 2003, the ITPB faced rising concerns about the privacy and security implications of adopting a wide range of technologies. Recognizing it did not have the necessary time or resources to address them all, the ITPB recommended that UCLA form a separate board to handle these specific issues. Based on the recommendation, Executive Vice Chancellor Neuman formed a new Board to advise exclusively on privacy and data protection concerns in 2004. Neuman charged the Board with two types of goals: some long term and visionary, others short term and operational. The mix of goals became a central characteristic of the Board; it attempts to fulfill them simultaneously, with varying degrees of success.

The Board regularly considered a range of values in its deliberations and recommendations. Maintaining flexibility helped the Board balance its visionary and operational duties and goals. Occasionally, operational duties dominated the Board’s focus, often because, although the Board originally reported to the Executive Vice Chancellor and the Chair of the Academic Senate, in practice the Senate had minimal formal involvement until recently. Thus,
the Boards’ orientation has tended to take on a more administrative cast. The Senate’s values and
interests are represented indirectly by the input and active participation of the board’s faculty
members, who are themselves Senate members and tend to share and represent the Senate’s
values and priorities.

Unlike the ITPB, where faculty membership predominates, membership on the Privacy
Board comprises even numbers of faculty and administrative members, plus one undergraduate
and one graduate student representative. The Provost and the Academic Senate jointly appoint a
faculty chair. Representatives rotate occasionally but many current members have sat on the
Board since its inception. As a result, many Board members have developed a kind of shared
language, and often anticipate each other’s positions based on their long-term Board service and
the viewpoints and values the members hold. Typically, the Board meets once per quarter, with
agendas reflecting the dual visionary and operational aspects of its charge, as well as ongoing
institutional issues and challenges. For example, the group completed and released its final draft
of UCLA’s Privacy Statement in 2011, but continues to engage in high-level discussions about
the principles it represents and their application in practice. Additionally, the Board advises on
particular privacy or data protection issues or controversies as they arise, whether major or
minor. In all these activities, the Board expresses and applies UCLA’s institutional values—not
just in policy, or in its advice on applying those policies or various controversies, but also in its
stable organizational structure, membership, and continuing work.

The Privacy Board was also the first body of its kind in the UC system, and among the
first in any U.S. university, according to a founder who had searched for comparable governance
structures during the planning processes. Thus, it has served as a model for value- and mission-
driven IT policy governance. The Board’s original formation, in response to the ITPB’s sense
that privacy and data protection warranted greater attention among campus policymakers and the
values of the ECP, has also encouraged the expansion of its principles beyond communications records to other business records and data sets as well as campus IT services. Applying rigorous privacy standards beyond communications records has had wide-reaching effects on nearly all university technology practices.

The Board differs from other IT governance committees. Like the ITPB, it shares representation, but has only an advisory role. It differs from other operational and strategic technology groups on campus because of its visionary responsibilities. To fulfill these, the Board produced a set of privacy principles with broad implications for the campus and, ultimately, the UC system. The Board accomplished this policy recommendation while also hearing and debating pressing issues, vetting technology-adoption proposals, and discussing the potential consequences of emerging technologies. Overall, the Board exemplifies UCLA’s distinctive approach to IT governance: mission-driven, value-informed, and cooperative. The choice to follow the shared governance tradition shows how policymakers understood, at an early stage, that information privacy is a necessary condition of academic freedom, and those who have a stake in these institutional values should be fully involved in decisions about the resources and infrastructures that reflect them.

**Values in Practice**

Beginning with the Board’s namesake value, privacy is the right to be let alone (Brandeis & Warren, 1890). In the United States, this right is recognized as part of the right to property, both tangible and intangible. In an academic institution, privacy is also necessary to ensure intellectual freedom values. To secure those values and exercise those freedoms, individuals must be able to trust the institution to protect them.

[Academic and intellectual] 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 these values possible. (UCLA Advisory Board on Privacy and Data Protection, 2010, p. 2)

In the context of digital information, privacy protects people’s ability to conduct activities without observation, and to control information about them. The Privacy Board established two types of privacy recognized by the university—autonomy privacy and information privacy—as organized in Figure 3 (UC 2011, p. 5).

Figure 2: Privacy types

The Board categorized and defined privacy types while writing the university’s privacy principles. During this process, the CPO drew the diagram, which evolved along with the conceptualization.\(^8\) According to the diagram, autonomy privacy is the “ability of individuals to conduct activities without observation.” Autonomy privacy protections guard activities like search-engine queries, Web traffic, and research against surveillance and monitoring. Privacy means the “individual privacy” protected by the ECP, linked to academic freedom and civil

---

\(^8\) This version of the diagram was the standard for several years; it appears in privacy statement draft resources, including the initial references used to draft the UC privacy statement, discussed later in this chapter. At the time of this paper, the CPO is beginning to use a revised illustration that better captures the relationships, one that will likely become the new standard.
rights. Information privacy “protects information about individuals.” Information privacy protections govern the dissemination of information about individuals, such as Social Security numbers, heath records, student or employee records, and financial information.

The university also recognizes information security and IT security. Information security concerns the protection of infrastructure and information that could compromise confidentiality, integrity, and availability of information. Information security excludes individuals’ activities but includes information about individuals plus other types of information. IT security specifically protects the technical infrastructure necessary to support collecting, storing, and sharing information.

UCLA developed these definitions over time, and though they are commonly used now, specifics varied in the past. An interviewee pointed out that in earlier versions, the diagram did not include the IT security layer; without the physical components, the diagram kept focus on privacy and security concepts. This is another minor example of the Board’s separation of visionary and operational goals, though in the end, they were both represented. The act of delineating and defining privacy and security concepts was a fundamental contribution to university policy, and is an important part of the Board’s history.

Since 2004, the Privacy Board has maintained its core privacy values but has addressed them in different ways. It also worked to understand those values in the context of technological process. As it has continually negotiated the balance among the set of institutional values and responsibilities, certain aspects of those values have fluctuated in importance. This is obvious in some examples. For instance, as mentioned in Chapter 2, outsourcing an e-mail service requires careful attention to privacy concerns in light of the vendor’s security measures. In contrast, in a system breach, the importance of security measures comes to the forefront, sometimes to the detriment of scholarly communication. In other examples discussed later in this chapter, the
advisory responsibilities of the Privacy Board have required a nuanced balance of several values at once. The ability to adeptly address complex issues did not happen quickly; it took time for the Board to establish itself and find its place in the broader governance landscape.

From the start, UCLA administrative and academic leadership acknowledged that IT issues deserved careful value-driven discussion by a variety of the university stakeholders. A new governance structure was born, not simply because there was too much work for existing structures to handle, but because the university decided it needed a new body whose perspective reflected particular values. Other UC campuses (and other higher education institutions across the country) have primarily looked at privacy concerns from the perspective of compliance. They assess technologies and practices in terms of existing laws and policy. However, UCLA decided that these boundaries were insufficient for its needs. The university wanted to foster discussion not just about what it could and could not do under the law, but what it should and should not do. It wanted to look more broadly at its values and consider other ways to meet them in the present and future. So the advisory aspect of the Privacy Board has been a fundamental part of its function and identity: it is foremost a think tank (a term used by many interviewees): a collaborative environment geared toward evaluating technology strategy in the context of competing values and the university’s educational mission.

In the remainder of this chapter, I trace the history of the Board from the year before its charge through the present day, focusing on the major landmarks, challenges, crises, and decisions that have shaped the Board along the way through the voices of several long-term members. I also use several forms of documentation: meeting agendas, notes, and materials; internal and external memoranda; Privacy Statement drafts, presentations, and reports. Then, by synthesizing and analyzing this case-study data, I conclude with the argument that IT governance
is the active interpretation of institutional values and an essential component of UCLA’s policy context.

The Privacy Board’s Inception

Emerging Technology Challenges Privacy Values

By the early 2000s, the ITPB became increasingly aware of concerns about digital data privacy and security, particularly relating to the adoption of new communications technologies and record-management systems. Several interviewees remembered one particular emerging technology that served as an early driver. UCLA introduced the new BruinCard in 2003. It was a photo ID that controlled faculty, staff, and student access to buildings, services, point-of-sale systems, and debit transactions. During a final stage of rollout in April 2003, the administration made its use mandatory and a handful of ITPB members expressed concerns about the possible harmful tradeoff for such consolidated convenience. The group brought up these topics at the May 2003 meeting and decided members needed more details about the data stored, and its use and management. To address these concerns, representatives from the Office of Corporate Services and Controller attended the meeting in June to report on the limits of data collected and departmental access control.

An ITPB member recalls the root of the concern: when asked about who had access to the data, who owned it, and what the retention rules were, the Bruin Card representatives stated those operational decisions were left up to the individual departments. ITPB members who were already concerned about information privacy were mistrustful of decentralized management with little cohesive policy or oversight. Some declined to use the cards, despite objections of the administration. This became a small but important point of contention; the faculty holdouts did not mind protesting during meetings, but when the administration sent e-mails to faculty
mandating card adoption and singling out those who protested, they were upset. One faculty remembered the irony in this: “I’m like, oh this is really good for privacy. Just tell the whole world who is refusing to comply. We had a few good laughs over that.”

Eventually the administration issued the remaining faculty members cards. However, an interviewee suggested their capitulation was less a result of the university sufficiently addressing their complaints, and more that necessary services were inaccessible without one. Even in a shared-governance model, the administration can make executive decisions despite faculty protest, but must calculate the wisdom of doing so. Though cards were eventually mandated, the faculty gained enough momentum to question other privacy issues as well.

Interviewees frequently referenced the BruinCard as the Privacy Board’s catalyst, but committee records show a few other prominent examples. The use of Social Security numbers on campus and the Library’s technology policy audit were also contentious issues in early 2003, all of which came to the ITPB’s attention, particularly its faculty members. By that time, a small group of faculty began agitating around the idea that something needed to happen to ensure that the university properly and consistently addressed their privacy concerns. Each member had a different background, but each understood the high stakes of information privacy and its implications for academic and intellectual freedom. They were perplexed by the university’s apparent lack of foresight and its resistance to properly consider privacy in technology strategy. Several interviewees recalled a period of frustration when they sensed pending trouble, but their colleagues were disinclined to recognize it or make substantive changes. It did not take long for those ITPB members to coordinate their efforts and strategize. “And I began to agitate around [asking] why doesn’t UCLA. … Why isn’t it worried about privacy issues and academic freedom issues and all of those things surrounding that?”
Once a small group began working toward a shared purpose, they explicitly traced the lines between information privacy and academic freedom, and convinced their colleagues to give them immediate attention. At this time, ITPB members showed a disparity of interest in potential privacy issues and their implications and willingness to vocalize concerns. According to interviewees, committee members had different impressions of the group’s collective privacy awareness at the time. Some credited the ITPB for paying any attention at all, and recognizing the scope of the problem.

There were a couple of things that really drove the point home to the ITBP, that privacy, not only was this something intuitively that was important, but that was going to be so big they couldn’t possibly take this on themselves. And they foresaw, as they sometimes do, that they really needed to pay attention to privacy.

Another was surprised at a lack of privacy awareness on campus, particularly in light of government overreach in the Patriot Act’s early years.

I was on the [ITPB] and I kept asking these around the corner questions about well—that’s an issue of privacy. Where do we deal with privacy at UCLA? Because I had worked with my general counsel at [another library] pretty closely because we were getting demands to deliver either computers or documents or whatnot under federal summons agreements.

Administrators realized that they could more effectively cope with new legislation if they had a strategy, or could convene a group of decision-makers.

And that was the first time we had to deal with that new data breach statute—is what I think it was, and that’s another that we had to comply with. And I don’t know if that was part of the thinking, that gee, it would have been nice if we had had a board that we could run some of these ideas by. That was a challenge, working through that and deciding if it was a breach, and what do you do about it, and who do you notify, and that was … not fun.

Technological advances like ID cards and centralized records certainly were not unique to UCLA, and neither were related privacy challenges; many other higher education institutions were confronting the same problems. However, UCLA took a conceptual path that led to very
different outcomes. The critical point was when faculty and administrators decided that privacy policy should not stand on its own because of the relationships between privacy and other institutional values. Policymakers saw the tension between privacy and transparency in public records. They could see tension between privacy and open access in the pursuit of academic freedom. They saw its role in everything from compliance models to campus security. The choice to build a set of privacy principles to uphold institutional values across the university mission set UCLA apart from other institutions, setting the stage for a holistic approach that naturally fit into a shared-governance model.

Proposing the Board to the ITPB

UCLA’s shared governance structure allows for distributed responsibilities, but even administrators tend to take academic approaches to decision making. This was true in the Privacy Board’s planning stages. It began with a small group of faculty, one of whom proposed the idea of a new governing body to the ITPB, prefacing the argument with a body of research.

I knew the lay of landscape and so I was coming in with a fairly academic set of principles for it so I was the initial privacy expert. But I don’t want to claim that it was me alone. It was a coalition of people and I had very little trouble getting people to join up and get on my train at the time.

And to get the background for the Board I went to EPIC9 and I said what universities have privacy officers, and what universities have boards, and they could only find a couple universities that had anything comparable at the time. And they gave me a student intern … who also did a good bit of background digging for us. So by the time we were ready to make a formal document, you know, four corners. This is what we wanted to do, we had a really solid piece of evidence together, and we were really talking from faculty concerns rather than from the administrative ones because it was. … We had such an easy time getting faculty engaged.

9 The Electronic Privacy Information Center (EPIC) is a Washington D.C. based research center that focuses on emerging privacy and civil liberties issues.
Once the groundwork was prepared and received sufficient faculty support, the ITPB approved an additional proposal to UCLA’s Academic Senate and the Executive Vice Chancellor in February 2004.

Jim [Davis] and I led the charge on getting this started, again and by having faculty and administration working together, and of course he is faculty, and administration at the same time. At the time, and [ITPB Chair Chris Foote] was very much on board with that as well. So the three of us, we then, met with Academic Senate leadership to make a pitch and we met with the EVC at the time who was umm… Dan Neumann to make the pitch that we wanted. … That these issues were not only. … There were big enough to start swamping not just ITPB, but UCLA.

From this founder’s point of view, early success was a result of preparing ample background, framing the issues, and establishing baselines while demonstrating need.

If we had come in and said, “We are a bunch a privacy activists and we think that UCLA should do this because …” You wouldn’t get a lot of traction with making up our own rules and what we thought the principles should be … [but] we could come in and say here’s a bunch of international treaties that have many national laws and then have laws and regulations within this country that are based on these international agreements and we’re proposing that those agreements, those principles be adapted here for our record-keeping systems. This will put us in a much safer and more principled place then we are now. This will protect us, it will allow us to be proactive; it will also protect us from certain risks and liabilities because we’ve got something solid to stand on.

By rooting the proposal in international standards, the proposal drew legitimacy from established sources and demonstrated the benefits of focusing on privacy issues.

The time and place aspects of this case are important. A small group of agitators ignited a privacy-based movement that was critical to the Privacy Board’s inception. They advocated a proactive approach, rather than a reaction to crises. They wanted to think about values and principles before making policy.

Because we’re the only ones to build a board like this. A lot of things were just the right people in the right place at the same time. … We had a critical mass of like-thinking people who showed up at the right place at the right time. … I think there is a critical mass at other campuses, but they haven’t had the catalyst to bring them together.
The ITPB’s Recommendation

In the summer of 2003, ITPB appointed a Task Force on Privacy and Data Protection to make action recommendations to the ITPB about the scope of work and membership for a proposed Privacy and Data Protection Board. In September of that year, the Task Force submitted a recommendation for the formation of a standing committee that bridged academic and administrative lines, keeping with the universities’ shared governance tradition (Foote, 2004). A faculty interviewee stressed UCLA’s commitment to shared governance:

I don’t think any other UC campus has something like this. There are very few boards that engage faculty and administrative governance around the policy the way UCLA does. I think that has a whole lot to do with the climate that this comes out of. And that really echoes into the difference between our approach and why UCLA ended up being the real core at the system wide leader, because we invested early.

The Privacy Board’s Charge

The Charge

The new Board’s charge specified four responsibilities. Two were deliverables, whereas the others were longer term tasks. The group was asked to (a) establish high-level principles for UCLA that were consistent with the fair information-practices guidelines established by the OECD; (b) articulate other IT policy principles that would reflect the institutional values and cultural expectations of the University; (c) vet new records-management systems to ensure compliance with these guidelines;\(^\text{10}\) and (d) promote awareness in the UCLA community regarding privacy and data protection (Foote, 2004).

Given this broad charge, tension between goals was inevitable, and priorities have vacillated between vision and operations several times during the history of the Privacy Board.

\(^\text{10}\) Initially, the Board’s vetting duties were limited to records-management systems, but expanded over time to include other data.
Goal shifts occurred within the policy context, and the Board’s continuing efforts to balance visionary and operational objectives is a hallmark of its role and its influence on other IT governance structures, as explored below. Balancing is a major function of the Privacy Board and appears in the Board’s description.

The UCLA Board on Privacy and Data Protection (“the Board”) is the campus nexus for consideration of institutional privacy and data protection needs, when these needs must be balanced with the campus’s many other values and obligations—for example, innovation, openness, accessibility, transparency, operational effectiveness, ethical behavior, and administrative and legal requirements—and account for external trends in technology and individual expectations. (UCLA, n.d.)

During the Board’s initial planning stages, the founders were aware of the limited resources available, and restricted the range of its decision-making responsibilities. An interviewee explained that in lieu of a proactive comprehensive IT system overhaul, the group focused on new systems or those scheduled for review.

We knew we could never get the staffing to go back and unpack every records management system on campus, that was just way out of scale, but as people developed new systems and were asking for funding and resources to do big changes, that’s the sweet spot when you can force them into review.

Once under review, the Board could take the time to “sensitize them to the code of fair information practices” and encourage decision makers to include those practices in their strategy, including considerations such as data collection, retention, encryption, and access restrictions.

**Membership**

Initially, Executive Vice Chancellor Scott Waugh chose the faculty to serve on the committee, and chose administrative staff members who already had privacy-related duties. When asked if it was a difficult decision to set the scope of the charge to create a very large and diverse committee, a founding Board member replied:
No, it seemed like an obvious one because we were modeling it on ITBP. So ITPB was already intended to get a broad base and consensus. So similarly, we wanted to get some administration on and we certainly wanted [Vice Provost Jim Davis] and [Director of Strategic IT Policy Kent Wada’s] position which was much more nascent.

We wanted to get, certainly a mix of social science and law. I’m not sure we got as much technology was we might have although there is a cryptography guy, a couple of cryptography guys we invited, but getting them to show up … because crypto is not the same as privacy.

Early Board documents show that the Board left space for an external privacy expert but it was not filled because internal members provided the necessary expertise.

Not all members were immediately obvious choices, but joined as their duties brought them into the Board’s path. One IT employee first brought an issue before the Board, then joined and brought a valuable perspective to the campus from previous work in government, where employees have no expectations of privacy:

I was getting used to this job where I couldn’t do what any other CISCO could do. And I brought up the case and [Vice Provost Jim Davis] said this sounds like a really interesting board to be on, essentially because I’ve given up essentially every privacy right I’ve ever had.

That experience was a good fit at UCLA, because it came from an employee with experience in a value-based institution with vastly different methods. The CISCO also brought many operational issues before the Board, challenging UCLA to balance ideals with practicality and articulate its policy positions.

A few interviewees stressed the importance of broad representation as a way to protect varied interests, and center decision making on academic values. They pointed to a focus on the community as a whole. The Board encourages faculty, staff, and students to advocate for their interests. Diverse representatives underscore the notion that IT policy serves a wide community and the common good. Many Board members commit for several years, adding an element of cohesion.
And I think in part it’s because as experience goes on, and one of the great things about this board is that most of the people who are on it have been on it since the beginning, and so there’s great cohesion and great understanding of how to talk, almost in shorthand as people who have worked together a long time tend to do.

An interviewee recalled that initially, members worried about including a Medical Center representative, because the Center operates under more stringent privacy regulations than the rest of campus. However, ultimately, that member was not distracting. The Privacy Board found that health-data concerns were not a barrier to healthy discussion. In fact, the Medical Center’s privacy expectations encouraged the campus to consider its own standards, as well as providing reasoning for deviating from those standards. It also encouraged the Privacy Board to consider how local privacy policy is established and implemented.

**The Board’s Role in UCLA’s Governance Structure**

The Board reports directly to the Executive Vice Chancellor and has additional relationships to other decision-making groups on campus, as shown in Figure 3. The Board interacts with the ITPB in matters of strategy and when issues require “wider discussion or more formal campus endorsement.” It works with the Oversight Committee on Audit, IT Governance, Compliance, and Accountability when privacy or data protection issues have “institutional risk or compliance implications” (UCLA Advisory Board on Privacy and Data Protection, 2013a, p. 1).
Figure 3 is not entirely consistent with the original charge, which indicated that the Privacy Board would report to the Executive Vice Chancellor and the Academic Senate Chair. However, after the Board formed, the Senate took a different role than originally intended. Figure 5 reflects the reality of UCLA’s governance structure; the Board primarily reports to the Executive Vice Chancellor, with minimal Senate involvement (though the Senate has been more involved recently). An interviewee recalled some “hot discussions” about to whom the Board should report; the respondent insisted it should be the Provost and the Executive Vice Chancellor because they are the chief academic officer and chief administrative officer, respectively. But although it was important to establish those official relationships, they have “never been overly worried about who do we report to because none of us are very bashful about speaking out. So when we felt strongly about something, that got expressed.” Occasionally, the Board escalated issues to the Provost or the Executive Vice Chancellor when it could define, frame, discuss, and assess risk, but did not have (or want) decision-making authority.

From the beginning, much discussion (and some disagreement) ensued around the Board’s role, which is primarily advisory but in some cases operational. The degree to which the
Privacy Board realizes that operational role has been a subject of some contention. The Task Force appointed by the ITPB first considered creation of two separate boards with advisory and operational functions, but in the end recommended forming “one advisory board with broader responsibilities” (Foote, 2004, p. 1). One faculty interviewee wanted the Board to have more authority, but scaled back efforts in the planning stages to ensure a smooth Senate endorsement.

**Scope and Scale**

As discussed above, the Board’s charter included visionary and operational goals: establishing privacy and other IT principles as well as vetting campus IT systems. The Privacy Board’s role reflected that duality. It was intended from the start to be an advisory board. Particularly in the early years, while it was establishing itself and drafting privacy principles, it made sense for the Board to operate at what one interviewee referred to as the “hundred-thousand-foot view level.” By attending to privacy and data protection issues as they emerged, the Board eventually “[came] down to a fifty-thousand-foot view level, so that [it is] remaining very strategic for the institution, but coming a little closer to the operational stuff.” Some Board members have favored expanding its discussion-focused advisory role from the beginning, but it has been a contested topic, not formally addressed until years later. Though the Board does occasionally make judgments, it does not have the authority to implement or enforce decisions on its own.

**Perceptions of Early Successes and Failures**

Interviewees had varying opinions about the Board’s success, but most agreed progress was slow. A faculty Board member was critical of the time it took the campus to recognize it as a valuable resource.
I would have liked us to disseminate what we were trying to do sooner. And things were moving so fast, you think now; there was no such thing as MySpace or Facebook when we started this. There was no such thing as, I guess mobile phones were early but there was no such thing as smart phones. So we were seeing this coming. We like to think we were pretty prescient, that we saw the tip of the iceberg. I think if we had gained more visibility and reached out more broadly earlier, we might have headed off a few problems.

That interviewee blamed a lack of “mandate and presence” for not being proactive enough. In the first few years, Board members knew they should reach out to IT groups, but were not ready to be a resource.

And it was that lack of anything to point them to, saying “this is why you should come here, this is what we are about.” … All we had was that charge statement. And now we’ve got various other documents and it’s much more clear about who we are and what we are doing.

Another interviewee remembered that the early lag caused some issues that were appropriate for the Privacy Board were brought to the ITPB instead because it was able to move more quickly. It took time for the campus to know the Board was a potential resource.

I think where we didn’t move as quickly as some of us would have liked was in getting a presence. So it took a long time to get the website up, a long time to get some policies out and disseminated. Where if we had promulgated what we were trying to do more quickly, in fact the kind of procedures that we were trying to get in place, might have prevented the big data breach.

However, the Board was able to handle some pressing problems more efficiently than others could. An interviewee said that although it took semesters to establish privacy principles, the Board responded quickly to pressure from the entertainment industry regarding illegal file-sharing. Over time, the Board gained its footing and became more efficient.

Key Operational Issues

The Board often exercised its capacity to consider conflicts between institutional values and apply the balancing tests encouraged by UC. Input from the Board demonstrated nuanced
approaches that weighed interests and encouraged cooperation among decision makers. Several issues were operational in nature, ranging from interpreting law and UC policy to local implementation. The Board frequently discussed developments in systemwide policy, such as ECP revisions in 2005, e-mail policies in 2010, and the UC Privacy and Security Initiative from 2010 to 2012. It also worked on several campus-specific issues in areas of research, data protection, records requests, and data retention, a few of which necessitated ongoing dialogue.

**Illegal File-sharing**

Illegal file-sharing, especially among resident students, was among the first issues the Board considered. I discuss file-sharing at length in Chapter 4; however, it garnered significant attention from the Board, which discussed it regularly through 2009. The Board was instrumental in developing UCLA’s campus-wide strategy, as well as articulating privacy values when defending the strategy against external stakeholders. The Board strongly supported academic freedom values, and vehemently argued against any action that would inhibit UCLA scholars’ free inquiry.

**Privacy and Academic Freedom in Research**

A few interviewees remembered when the Board “became infinitely aware of the intersection of privacy and the IRB and the issues that would come before each of those bodies.” In 2005, the IRB received a proposal from a doctoral student researcher in the computer science department for a project that would analyze Google searches on campus networks. The researchers’ advisor also approached the Privacy Board to ask for permission to use campus domain-name-service records and search history logs. During its January meeting, the Board carefully considered the conditions and context, but ultimately decided the research mission did
not outweigh privacy values related to free inquiry and rejected the request (UCLA Advisory Board on Privacy and Data Protection, 2006).

The Data Security Breach

The large-scale 2006 data breach mentioned in Chapter 2 stunned the campus and had long-term implications for the Privacy Board. The Board devoted that month’s meeting to the topic, discussing the breach, the notification process, and actions taken. After that, the Board returned to information security topics in nearly every meeting through 2008. Mostly, the Board was briefed on security strategy and policy. However, in 2007, it also evaluated specific networking practices such as scanning, analyzing network behavior, and virus versus content scanning. The Board took the opportunity to discuss ways to balance institutional values in a policy environment that had shifted to privileging information security because of the breach.

Contracting Cloud Services

The Board discussed several cloud-service issues mentioned in Chapter 2. Members voiced some of the same concerns as they had in 2003, but those concerns expanded beyond the institution to include third parties. One significant example of this expansion was UCLA’s partnership with Google, where the Board attempted to reconcile administrative strategy with institutional values. The sequence of events was quite similar to what had happened with the BruinCard. First, university administrators announced a strategic decision, this time to outsource university e-mail to Google. Administrators stressed the benefits of cost savings and increased functionality from bundled applications, unlimited storage, and lifetime UCLA e-mail addresses. However, interviewees thought the plan had progressed too far with too little input. Board members familiar with Google’s business model knew that Google offered services in exchange for the chance to advertise to account holders. To create targeted advertising, Google scans
e-mail content, a direct violation of the ECP. An interviewee recalled trying to disseminate information about privacy dangers: “I really did try to stop them; I really did think it was a bad idea.” The respondent expressed surprise that even some privacy-minded colleagues supported outsourcing despite warnings to be suspicious of Google’s motives. This respondent was also concerned about the legal implications of off-site third-party hosting in cases of subpoenas, warrants, or records requests, but knew that security and transparency issues did not incite the response that privacy concerns did; thus, the interviewee chose to “play the privacy card” to gain attention.

During these discussions, it was clear that faculty did not always know the implications of using non-university e-mail services. An IT security administrator relayed common misconceptions:

Because they know that the ECP protects them, right? But if a [Public Records Act (PRA)] gets filed, that’s actually public data they have, and they’re subject to a PRA. So they’re kind of in this quandary. And I’ve actually heard a professor say, “Oh a PRA doesn’t affect me because I use Gmail.” Umm … it’s still the universities’ data, and you shouldn’t have it out there. But they just want to get their job done and make it easier and a lot of them are not tech savvy.

After the UC’s Cloud Computing Task Force published its report in 2010, the Board’s discussion of third-party services continued. In 2013, the ITPB requested the Board’s input regarding the upcoming deployment of several cloud services for mail and collaboration, including Google Apps, Microsoft Office 365, and Box. By this point, UCLA had negotiated agreements with each of the services to provide “generally a more balanced alternative to consumer grade cloud services that lack the protections of the negotiated contractual terms” (UCLA Advisory Board on Privacy and Data Protection, 2013b, p. 1). One important concession included participation; UCLA offered departments and units the opportunity to make a case for opting out of any particular service if it did not fit their needs, such as for protected research
data. The Board attempted outreach regarding acceptable data use for each service, but as mentioned in Chapter 2, it is a difficult task to educate the whole campus community.

**Opus**

Opus is a web based electronic-record system for UCLA faculty that is currently in the final stages of development under the direction of the Office of Academic Personnel and the Vice-Chancellor for Academic Personnel. From the outset, it was presented to faculty as an administrative attempt to improve “efficiency, transparency, and accuracy of the academic review process by replacing current paper files with a secure electronic profile, a convenient and automated review process, and robust messaging and reporting features” (“About Opus,” n.d.). The Opus repository includes electronic curriculum vitae, an academic action tracking workflow and review, reporting-decision support, and data syndication.\(^\text{11}\) From the start, the centralized nature of so many data points raised privacy and appropriate-use issues among faculty across campus. Many Opus-relevant records were already public, but had been collected and stored inefficiently, allowing for limited contextualization. Meaningfully comparing data with disparate origins can be difficult, but when that data is gathered into a centralized database, formatted similarly, and searchable, entirely new analysis is possible.

Opus was sponsored by administrators, who in 2011 convened the Faculty/Senior Staff Oversight Committee for the Electronic Dossier and Review Initiative, charged with providing guidance for system design, integration, interface development, use of qualitative data, privacy policies, practices, and training. The administration framed the single faculty-record system as a move toward more transparency and consistency in faculty-related decisions. Overall, faculty responses varied somewhat; some saw Opus as a tool that facilitated administrative functions

\(^{11}\) In Opus (as in other systems), data syndication involves consolidating and synthesizing data from multiple sources so that it appears consistently across applications, increasing access and potential usage.
over academic benefit. Some objections were based in more specific reasons. For example, the Board pushed back regarding the appropriate use of included records, particularly those that had been initially gathered for other purposes. Those concerns followed a familiar pattern; members wanted more information about how and what information would be collected and how it would be controlled, used, and accessed. The Board heard an introductory briefing from administrators and discussed concerns in their May 2012 meeting; some members felt this step should have occurred much earlier in the process, and would have if the Board’s existence and function were more widely understood, particularly among administrators (UCLA Advisory Board on Privacy and Data Protection, 2012b). An interviewee recalled the events of that meeting:

I think [the Opus coordinators] were sort of brought to us and told that they really should talk to the Privacy Board before they got too much. … Because they were already in quicksand. And we again started asking them very basic code of fair information practices questions about what were they collecting, why are they collecting it, and, what was the retention plan, and the access plan, and the use plan, and all that and they had never heard of the OECD principles. They had not thought about some of these … these very basic principles, they thought of them in a very isolated ad hoc way. … They weren’t doing big picture. So the fact that if people knew [the Board] existed sooner, I think we might have saved a lot of people a lot of time.

Not all faculty concerns directly related to privacy, but existed alongside it under the broader umbrella of data use and stewardship. The faculty argued over the “appropriateness” of the included data, such as information that could be used to automate productivity assessments or public-records requests. The potential for algorithms to replace nuanced human interpretation regarding complex issues of information sharing and disclosure caused a significant amount of consternation among Board members.

This type of skepticism echoed broader themes that emerged inside and outside institutions beginning in the 2000s. The rapidly increasing ability to collect, store, and analyze huge data sets about behavior was and remains one of the most contentious technological advances in recent history. In higher education, institutional culture undergoes significant shifts
when big data come into play. The Board called for clear policies regarding appropriate use of

data early in the decade (discussed at length later in this chapter). This advocacy clearly

indicated two things: The Board’s ability to foresee problems not yet universally acknowledged,

and efforts to address those problems before the university implements the technology.

The Board last discussed Opus in October 2012, when project leaders briefed members

on policy progress. The presenters classified Opus data in three privacy-related categories:

information already public, information not available publicly but not protected as private, and

protected private information (Goldberg, Zimmerman, & Buzzi, 2012). Opus would limit the
default display of data in each category; for instance, it would display publicly-available

information such as job title and publications but not publicly-available salaries. No private

information would be displayed by default, but the group had not yet decided display status for
data that was neither publicly available nor protected. Opus would also make available reports

containing non-identifiable aggregate information that were already required by government and

policy, but the group had not yet determined a policy or process to govern the many possibilities

for ad hoc queries that would be possible, particularly whether or not those reports would be

available in Public Records Act requests. At that point, faculty still had many concerns about

privacy, but their voices were losing influence. An interviewee recalled that during the October

2012 meeting, an administrator argued that the university was past the time for further

negotiation about “granularity or faculty permission.” Despite remaining objections from Board

faculty, Opus was initially launched in February 2015, with a timeline for optional use after July

2016, and required use after June 2017.

Restructuring the Board

In light of the many operational issues facing the Board, some felt that its large, varied

membership hampered its ability to be sufficiently responsive. Thus, in the March 2012 meeting,
the Board’s leadership proposed forming an executive subgroup for more rapid and detailed decision making. The problem was primarily a matter of logistics and resources; gathering the 15 members once per quarter was difficult. Additionally, discussion takes time. The group regularly analyzed several perspectives, but did not often vote on specifics; an interviewee suggested it was easier to get participation when only asking for advice. Gathering increased input would be arduous, and possibly outside the scope of the original charge.

In the meeting, the group “agreed in principle to reorganize to move from our current ‘think tank’ mode to an operational mode” (UCLA Advisory Board on Privacy and Data Protection, 2012b, sec. B) UCLA’s Oversight Committee on Audit, IT Governance, Compliance, and Accountability approved that proposal and at the May meeting, Board members discussed a roadmap. The Board took a significant step by creating a CPO position, which was in the original charge but had been set aside. Creating a position exclusively for privacy issues was unusual for a university at that time, even in the UC. Creating the position was partly symbolic and partly practical. The Privacy Board felt the duty to “recognize the parallel nature and importance of privacy relative to information security … [and] recognize the broad sense of the term privacy” (UCLA Advisory Board on Privacy and Data Protection, 2012a, p. 2, see Appendix C). An interviewee remarked that in addition to the symbolism, having a dedicated employee meant an expert could make day-to-day operational and administrative decisions that could reflect the Board’s advice.

In 2012, the Board also considered changes to its structural arrangement and a formal decision-making process. Leaders proposed forming an executive Privacy Board committee to address the responsiveness problem. Suggested members included the Chair, an ex officio member, the CPO, and the Vice Provost of Information Technology. The committee would have the authority to take action as well as consult. An interviewee explained the reasoning: The
Privacy Board could not manage a crisis like a data-privacy breach, but a smaller administrative group could. Transparency and integration into campus governance were also a part of this movement. The Privacy Board discussed more public-facing documentation and seeking endorsements from the ITPB, the Provost’s office, the Council of Deans, and the Senate Executive Board.

**The Visionary Mission**

**Developing Privacy Principles**

The Board worked on privacy principles from 2004 to 2011. Its objective was to reach beyond typical university models that focused solely on compliance or e-commerce approaches. The Board aimed to create a policy that would more closely fit UCLA’s institutional values and mission. It was a long process, partly because the Board was attending to other responsibilities at the same time.

From the start, members took an academic approach to the work. They began with OECD principles and the fair information practices presented to the ITPB during the Board’s original proposal, using them as a foundation. They also consulted with privacy expert Chris Hoofnagle to sketch the initial framework. A few interviewees remarked on what a good fit Hoofnagle was for the group; he had a solid philosophy and a gift for communicating the relevance of privacy values. The Board introduced this background at the second meeting in February 2005. By June 2006, the group had a first draft with the intention of completion by the start of the 2006–2007 academic year. That month, the Board circulated a document detailing what needed to be in the Privacy Statement. They argued a statement should “begin with an explanation of how privacy rights are grounded in academic freedom,” then move to the relationship between technology and academic freedom, as well as other university values. It should also “recognize that intellectual
freedom could be limited in an environment where individuals’ actions are under surveillance.” Additionally, it should address the tension between openness and privacy, arguing that “it may be by focusing efforts on protecting personal information while not hindering research or the freedom to publish” (“Campus Position Statement on Privacy Draft Version 1,” 2006, p. 3, see Appendix D).

After this promising start, further work on the statement stalled for nearly 2 years. In the intervening years, the Board attended to several other pressing matters. Privacy values first suffered from a lack of attention in November 2006 when the university discovered the data breach, which marked the Privacy Board’s renewed focus and awareness of security issues. It also marked the beginning of a period of prioritizing operational issues over vision and principles.

Beginning again in the spring of 2008, the Board refocused on the statement and resumed drafting, releasing a new version once every month or two. That year, some members who believed the statement was too abstract proposed the addition of scenarios to guide implementation. Board members discussed the scenarios and added them to the December 2008 draft. That month, the Board approved a measure to circulate the draft for wider campus discussion and asked for input from the ITPB.

A working group contemplated scenarios in breakout sessions starting in November 2008. The group drafted two scenarios: Facebook and the BruinCard. Facebook was an obvious choice; through it, the authors could explore themes about visibility, disclosure, and privacy expectations using a controversial but ubiquitous technology. They also revisited the BruinCard, addressing further questions about how the data, particularly the photos, could be used for purposes beyond identification, like tracking. They discussed these scenarios for a few more months and included them in a publicly released draft in January 2009. Though unfinished, the
section on scenarios lasted through the March 2011 draft that incorporated the ITPB’s recommendations. However, when the draft was ready for campus release a few months later, the uncompleted scenarios were removed in favor of moving forward.

The Board finally released the UCLA Statement on Privacy and Data Protection for campus discussion in May 2011. In 2015, after approximately 11 drafts, the statement is still technically in the “campus discussion” phase, but with no plans for further revisions.

Interviewees had mixed feelings about the 6-year process of bringing the statement from bullet points to submission. Generally, they were pleased with the result but remembered feeling quite frustrated with the process.

We sat and talked about—what does it mean—we didn’t even know what it meant and what was covered and we spent a lot of time coming up with what was our privacy principle. … But for years, that was a draft, and it was sitting up on the website as a draft.

Even one of the most fervent advocates of privacy values remembered the process as somewhat excruciating:

I saw that blasted draft thing—so many times I thought I was going to puke. To be blunt—it was just beating the governance ideas absolutely to death. I mean, give me a break! Let’s get on with life here.

However, the delay was not all bad, as this was a case of learning by doing. As the Board addressed each of the operational issues mentioned above, members developed the language to discuss what they were trying to do and why. Over time, their perspectives and conceptualizations matured, contributing to a more robust statement.

Value-Based Language in the Privacy Principles

The Privacy Statement drafts offer a look into the development and articulation of the privacy principles and their implementation. Decisions about what to include, what to omit, the act of defining and explaining concepts, organization, and word choices all give a glimpse into
the intellectual endeavor. Through them, it is possible to trace the conceptual development of privacy at UCLA and see how it reflects institutional culture and operates in the broader policy context.

In the May 2010 draft of the UCLA Privacy Statement, the group made a few important changes to Appendix A. In previous drafts, Appendix A was titled “Guidelines for Implementation,” which is standard language for policy documents. In the first Release Candidate draft, the authors replaced the word “Implementation” with “Attainment.” In the following paragraph, they changed the language about “implementing the Privacy Statement” to “attaining the principles.” Additionally, the goal of the guidelines changed from “resolving conflicts” to “achieving an appropriate balance” (UCLA Advisory Board on Privacy and Data Protection, 2010, p. 4). These small revisions make the point that this document is not policy, but an articulation of values. The statement does not give rules for the university to implement, but goals to attain.

Another noteworthy revision occurred between the May 2010 Release Candidate and the May 2011 Campus Discussion version. In the statement section, a change in the language clarified UCLA’s conceptualization of institutional values. The earlier draft had this statement:

UCLA must balance its respect for privacy with other values that it esteems and with its many legal, policy, and administrative obligations. (UCLA Advisory Board on Privacy and Data Protection, 2010, p. 2)

In the next version, this paragraph replaced it:

UCLA recognizes that there is a constellation of values and of legal, policy, and administrative obligations that are always in play. Privacy is an important condition threaded throughout this constellation. (UCLA Advisory Board on Privacy and Data Protection, 2011, p. 2)

The “constellation of values” concept has a history primarily in academic literature, particularly in the social sciences and law. It has not been common in UCLA’s policy, and is a good example
of the academic nature of policymaking on campus. An interviewee recalled the desire to better articulate the forces at work in UCLA’s policy context. The earlier version indicated that the university need only balance values with obligations; the later version indicates a more complex environment.

**Guidance for Individuals**

Chapter 2 discussed UCLA’s efforts to educate its members about their privacy protections and their implications and its mixed results. The Board added another attempt to address education in the May 2011 draft of the Privacy Statement. The group expanded a footnote in former drafts to a new section entitled “Considerations for Individuals.” It encourages end users to manage their personal and business data separately.

> [T]he convenience of free or low-cost external e-mail accounts or other “cloud” services that store data outside of University control (and for which there is no institutional contract or agreement with the University) should be carefully weighed against the increased security, privacy and business risk in using such services. Each individual must take responsibility when making decisions about when it is and is not acceptable to use these free/low cost services. … While incidental personal use of electronic resources is permitted, any individual concerned about individual privacy unrelated to University activities should use a separate commercial account for non-University related electronic records and communications. (UCLA Advisory Board on Privacy and Data Protection, 2011, p. 8)

This was a well-intentioned effort to reach the larger community, explain the issue, and give advice. However, its impact remains uncertain; most employees are not required to read privacy policy and often do not seek it out until there is a problem. Nevertheless, the section’s inclusion provided a solid step toward making the Privacy Statement relevant to end users.
UCLAs Leadership Role in the UC Privacy Initiative

UC’s Steering Committee

While UCLA’s Privacy Board was drafting its statement, the UC also felt pressure to thoroughly address privacy and information issues, specifically the relationship between privacy and information security. In June 2010, UC President Yudof launched the Privacy and Information Security Initiative, charging a Steering Committee and Working Group with the responsibility of “perform[ing] a comprehensive review of the UC’s existing 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” (UC, 2013, p. 27).

The steering committee consisted of a broad cross section of functional areas in the university and included representation from faculty, staff, and students. Its final report, released January 2013, includes a UC Statement of Privacy Values and Privacy Principles, several recommendations, and an implementation timeline. President Yudof accepted the report, and after minor modifications, implemented it across the system. For instance, Yudof approved the recommendation to implement Privacy Boards on each campus, but rejected the idea of implementing a board systemwide to unite local Boards (though an interviewee pointed out that he did not reject the recommendation outright, but put it on hold).

Charge and Goals

The final report contains four recommendations. The first recommends that UC adopt its Statement of Privacy Values, the UC Privacy Principles, and the Privacy Balancing Process. The Privacy Statement declares autonomy and information privacy important values and obligations. The Principles give concrete guidance about the Statement. The 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.” Second, it recommends that each campus form joint Academic Senate–Administration boards similar to UCLA’s to

[Advise 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. (2013, p. 4)

The third recommendation is to establish a systemwide UC Privacy Board with the same duties, an attempt to unify the campus Boards. Last, the report recommends each campus designate a CPO “to be responsible for the collaborative development, implementation, and administration of a unified privacy program for the campus” (2013, p. 4).

The report was intended to propose “an integrated approach to privacy and information security.” Because information security policy was more mature at the time, the committee focused mainly on privacy to close the gap. But although it began with the intent of focusing on privacy, it “emerged with a more holistic, integrated view of privacy” and makes recommendations based on a “drive toward a unified privacy model led by the University’s mission and values” (2013, p. 3). This desire for a unified privacy model demonstrates growth by the committee, as it exceeded its own charge.

Several elements in the report echo themes found elsewhere in UC’s IT governance. The report included familiar themes of innovation and leadership; the committee saw that few universities had taken a holistic approach to privacy and information security. To correct that, the group offered its findings and its approach as a model framework for other higher education institutions. Like the ECP, the committee intended the statement to last, and intentionally did not mention specific technologies, recognizing that policy, principles, and values must outlive current technology infrastructures.
UCLA had a significant role in the steering committee. In an early meeting, the committee discussed a summary of UCLA’s Statement on Privacy, including the context in which it was created. The summary stresses the importance of the institutional mission and states, “We are a community rather than corporation; we are 24/7; we have everything that a city has, we are always fluid and changing; we all have multiple roles.” The committee identified four premises: (a) privacy, the right to be let alone; (b) confidentiality, not revealing sensitive information; (c) anonymity, the conditions of not being identified/identifiable; and (d) transparency: ensuring the community understands the “rules of the road” (e.g., social norms) (UC, 2011, p. 4).

By contributing a statement of community values and a governance model, UCLA’s representatives encouraged the path that UCLA took, particularly focused less on compliance and more on a broader conceptualizations of privacy interests. An interviewee recalled the difficulty of this process:

We had done a lot of work here already at UCLA. None of the other campuses had anything like this. … Because otherwise, because basically who they put on the committee were all the bean counters, all the administrative vice presidents of the university, who … they weren’t faculty, they weren’t students who understood the environment of the academy. They were worried about risk. And they could see no reason why they couldn’t look at anything anywhere anytime for any reason. And it’s taken, you know, you’ve got to move the Titanic around and try to steer it away from the iceberg when you’re working with UCOP [University of California Office of the President].

UCLA also contributed a faculty member to the Privacy Expert position, which was not filled at first. The representatives invited Professor Christine Borgman to make a presentation about the fundamental privacy principles, the issues, and the correlation with academic freedom values. Once the committee recognized the value of Borgman’s contributions, particularly as a faculty representative, they confirmed the appointment.
Therefore, it makes sense that the UC Statement of Privacy has only minor differences from UCLA’s version. As discussed above, UCLA revised the characterization of its policy context; using the “constellation of values … always in play” in place of language about balancing values and obligations. UC’s statement restores the original concept, stating that “the University continually strives for an appropriate balance” between several goals and responsibilities. (UC Privacy and Information Security Initiative, 2011, p. 14).

UCLA’s statement considers accountability and fairness, drawing on its fair information practices foundation:

There must be processes in place to ensure fairness where important decisions are made on personal data. There should be a mechanism for recourse for individuals who desire to challenge a determination based on personal information. (2010, p. 3)

UC’s Statement only mentions accountability but includes an employee-training requirement and commits to investigations of reported violations.

UCLA’s statement identifies principles of “sustainability and operational necessity” regarding the collection of personal information:

These principles should be applied in a reasonable manner so as to promote operational effectiveness (including appropriate security safeguards) while striving to design system that are sensitive to privacy risks. (2010, p. 4)

UC’s statement focuses more on “choice:”

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. (2013, p. 16)

UC’s statement also provides a way for individuals to review the information collected about them.

The UC statement includes a section called the Privacy Balancing Process, a “tool to guide decision-making when there are multiple privacy interests and University values or
obligations to consider, and no statutory provision, common law or University policy is directly applicable.” The UCLA statement, in contrast, does not mention specific implementation strategies and examples in favor of writing only a guiding document.

Localization

One reason UC rejected the idea of a systemwide Privacy Board was that the campuses were perceived to have too many differences among them to be supported effectively by an additional board. The UC Privacy Statement acknowledges this reality; the Privacy Balancing Process attempts to enable localized decisions. It was intended to “be employed by governance bodies … 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.” Its goal is to establish universal concepts as principles, but then let them grow and develop through practice into each campus culture. One interviewee mentioned the potential disadvantages of this approach.

Now you have 10 campuses that may choose to implement the same goals differently. And I think if you talk to some of the attorneys, they’ll tear their hair out going, “[you address] the same situation in two completely different ways and that can be used against us,” which, of course is completely true, but again, someone’s going to have to make a decision about what’s more important.

There’s going to be a huge amount of implementation that campuses are going to need to figure out—in some senses intentionally. Partially, the report was intended to make recommendations on a conceptual level, not necessarily about specific implementation, and partially because you didn’t want to go too far into the purview of each campus as to how to do things.

**UCLA’s IT Governance Landscape**

As summarized earlier in this chapter, the Board’s main purpose was as a representative advisory group, committed to evaluating the adoption and implementation of technology in the context of the institution’s values and mission. The Board, albeit unique in some ways, is
consistent with the rest of UCLA’s (and UC’s) technology governance. As a case study, it illustrates many of the prevailing themes in UCLA’s IT policy context: cooperation and collaboration, stakeholder buy-in, communication and deliberation, and the management of expectations and resources.

The Board is a noteworthy example of how the faculty and administration exert pressure on one another in a shared governance structure, with the faculty pressing for a stronger vision and the administration seeking to strengthen its operational role. The initial advocacy came from faculty members concerned by IT governance groups’ lack of foresight about looming IT-related issues. Those groups pressured the administration to take action, and the Executive Vice Chancellor responded by taking their recommendations and forming an advisory committee. The Board was born from an initial recognition that the university needed to address new technological issues in the context of university values. As an advisory group, its focus tends to shift to operational needs, particularly in times of crisis, but its values remain solidly in service of intellectual and academic freedom, which are supposed to take priority over managerial values such as economy and efficiently. When managerial priorities shift to make room for academic priorities, the influence of faculty interests in a shared-governance model becomes clear.

Shared governance also entitles an investment in process, of which a few interviewees were quite aware. With faculty and administrative perspectives (and generally several other more specific viewpoints) constantly in conversation, objections arose in response to any unilateral decisions, particularly those perceived as being mandated from above. Interviewees characterized the workings of campus IT committees differently: some describe them as cooperative or collaborative, others as oppositional. Some people will be dissatisfied with the results of the decision-making process, but few should be able to accurately claim they did not have a voice.
An investment in process means that policy at UCLA tends to be very front-heavy; a majority of the resources are necessary from the start. It is an enemy of efficiency, but most of the interviewees—faculty and administrators alike—seemed convinced that such a process makes for higher quality, longer lasting policy than the alternative. At least in theory, faculty and administrators supported the idea of building a solid foundation rather than making ad hoc decisions, and preferred to be proactive. Interviewees pointed to this attention to process, claiming it is one of the reasons they think UCLA is a leader among higher education institutions. The link may be accurate: The Board was a governance structure that needed to gain a good deal of momentum and emerge almost fully formed to be successful. Moreover, it was a groundbreaking approach that eventually influenced other institutions.

It is possible that the effects of the shared-governance model at UCLA are particularly pronounced because many administrators are current or former faculty members who tend to bring academic approaches to policymaking. This phenomenon is evident in the way the Privacy Board was proposed. The issues were clearly stated, thoroughly contextualized, and heavily researched. Additionally, an inclination toward orderly argument and heavy contextualization did not end with the proposal; it continued through the Board’s charge and into its inner workings, through the drafting of the Privacy Statement, and is still at work in the present day committee.

Consistent contextualization tends to lead to holistic approaches to problem solving, a theme to be explored in depth in Chapters 4 and 5, because it is evident across the cases in this project. This approach encouraged the university to consider privacy issues in the broader instructional culture and look at the relevant influences in the policy context. An interviewee explained the importance of multiple perspectives:

These are social problems masquerading as technical problems. And the technical people are more likely to come up with technical solutions, which may or may not. … The
technical solutions can help but you have to know where to implement them and fit them into the policy.

With this distinctly academic thought process, one can see how UCLA engages its technological issues in a much different way from institutions that take a more business-oriented approach. Following that, a broad view of issues calls for broad participation in decision making. When these factors exist in a shared-governance model, the shape of the Privacy Board is an obvious consequence.

The success of the Privacy Board is evident in its accomplishments, but also in the way it serves as a model for additional governance structures. Itself modeled on the ITPB, it became a model for a new group dedicated to data governance. By the time this new group was charged, the concepts and language used to describe IT-related values and processes of implementation were more established and familiar to everyone involved, perhaps expressing a natural progression in UCLA’s governance as a whole. Moreover, it was the inspiration for another committee that would further the university’s conceptualization of data, its values, and its appropriate uses, as discussed in the next section.

**Looking Forward: Challenges to IT Governance**

**Data Deluge and the Evolution of Data Protection**

As mentioned in Chapter 2, one of the ECP’s limitations was its focus on securing information assets such as computers, mobile devices, and infrastructure hardware, which are no longer the only (or most important) aspects of IT security. Until fairly recently, data protection was synonymous with information security. Concerns centered primarily on identifying and thwarting unwanted access; security measures primarily targeted data transmission. As information technologies have spread, the amount of information about individuals collected and stored has grown exponentially, and data have assets unto themselves, both valuable and
vulnerable. UCLA’s governance structure recognized this: The Chief Information Officer was also the Director of IT Security, responsible for protecting both physical assets and information. An interviewee mentioned that when the position was created, “most people [did not] see the difference” and it took years before asset and information security were more commonly understood.

As UCLA collected and retained unprecedented amounts of data, it needed to better understand the intersection of privacy, security, and data protection. Despite its full name containing “data protection,” the Privacy Board has tended to focus primarily on privacy issues, evident during the Privacy Statement’s draft stages: only in Version 4 did its title expand to include “Data Protection.” According to an interviewee, the authors were attempting to unite the concepts. However, an inspection of the drafts does not uncover any noticeable changes to the content reflecting the addition.

These are subtle indications of the campus’ natural tendency to focus on privacy issues first. The administration originally charged the Privacy Board with tasks related to records management, and the Board did address records systems on an ad hoc basis, though it was never a focus of the group. Nevertheless, since the Board’s charge, the university generated and stored progressively larger data sets while conducting business. Questions arose about the nature and life-cycle of data as well as its appropriate use, reuse, sale, and destruction. Board members and administrative staff recognized a need for a more developed understanding of data categories, policies, and practices. Eventually it became clear that these questions deserved more attention than the Privacy Board could commit.

**IT’s New Challenges**

As the concepts of privacy, security, and protection matured on campus and across the UC system, UCLA’s IT administration surmised that emerging concerns about campus data did
not fall entirely under the provisions in place. For any given piece or set of data, standards and practices were already in place to keep it secure and to keep it private. Although varying degrees of success emerged in these processes, security and privacy are governed by policy. However, a gap persisted existing policy and questions about data stewardship and governance. In these cases, the policy context directly shaped how the institution thought about its role and responsibilities in the data it collects and stores. By continually asking the question “we can do this, but should we?” a need for further reflection and possible decision making becomes clear.

Three particular issues surfaced around the same time and illustrated the existing gaps and foreshadowed others to come: governance issues, stewardship issues, and data-sharing issues. Although they are separated here for the sake of clarity, they significantly overlap and many data sets are affected by all three. The first example concerns learning analytics. Learning (or course) management systems (LMS), such as UCLA’s open-source CCLE collect large data sets about student behavior and performance. LMS logs calculate how often students log in, if and how long they engage with their course materials, and their performance on various types of assessment, among other items. Only the software limits the amount of measurable data. Educators can analyze course data for any number of purposes. For example, these data may link student behaviors with dates to completion, or provide information to instructors that can help them predict indicators of academic success. The analysis can benefit students. For example, if the analysis can identify high-risk students, the university can tailor its assistance programs.

Drawbacks to data-driven decision making include that learning analytics are fallible. If educators overlook critical data points or provide faulty analysis, teaching and learning can suffer. Despite their limitations, data sets generated by an LMS or other digital-learning tool are highly valuable. In 2014, the National Science Foundation awarded a grant to researchers at Carnegie Mellon to construct a new cross-institutional data-sharing infrastructure of learning and
student behavioral data. It will collect digital-interaction data, chat window dialogues in select classes and tutoring sessions, and affect and biometric data. The platform will be available to institutions as well as commercial vendors and for-profit organizations (Spice, 2014). Many institutions are interested, but UCLA has been hesitant about releasing student data to a third party, whose ultimate purposes or uses of the data are not always articulated, acknowledging that it raises ethical issues about student autonomy and privacy. Privacy proponents were worried about ownership with shared student data and the resulting aggregated metadata.

As with cloud computing, the problem with sharing data with third parties is that those agreements rely on the strength of data governance and stewardship, with some additional pressures. With third parties, it is difficult to ensure they will not only handle the data as they are contractually obligated (particularly security and privacy protections), but will uphold UCLA’s values when using or reusing the data. First, it is difficult to communicate the necessary governance measures in any official way, particularly because they have not been formally set yet in the institution. An interview participant gave the example of the difficulty of ensuring that a third party upholds a value like academic freedom. The second is the purpose of the third party. Any for-profit company has a purpose that differs vastly from the university’s mission. They may have no impetus to uphold UCLA’s mission in their own business model. In fact, even sharing data with other higher education institutions can be a problem, as their missions and approaches do not necessarily align.

The second example is Opus, the faculty record-management system mentioned earlier in this chapter. UCLA’s Book of Record Initiative launched in 2012 to support Opus’ data-gathering and management processes. Opus raised questions about several types of data that would be included in faculty assessment, such as the discrepancies in enrolment data among administrative offices. Opus captures class-size statistics in two different weeks of the quarter by
two different offices; questions arose about which would stand as the official record or which was the most appropriate record to use for this purpose. This discussion led to several others about the way the same data sets are handled by different units on campus. The university recognized that Opus’ success depended on academic and administrative users trusting the data. Rather than recreating data, Opus would rely on existing Books of Record to be well-managed authoritative sources. For that to happen, UCLA needed to systematically inventory and document available data to determine accuracy, then create policy and practices for effective stewardship. The Book of Record initiative intended to “provide reconciliation of the records of individuals on campus throughout the various systems” (UCLA Council of Faculty Chairs, 2013). Technical work included mapping and identifying data, integrating systems, documenting data lifecycles, and embedding metadata to create data transparency. To determine policy, the university needed to decide which data to include, locate authoritative sources, create an error resolution processes, and ensure ongoing stewardship (UCLA Academic Personnel Office, 2013). The initiative is still underway; inventorying campus data alone was a sizeable undertaking. The scale and complexity of the project has driven home the importance of a clear idea of who or what body can adjudicate appropriate-use conflicts.

The last example shares some themes with the other two examples, demonstrating how the complexity of issues around big data may necessitate a holistic data-governance approach. This case is about commercial providers of research analytics. In June 2014, the publisher Elsevier approached UCLA with a product they claimed would capture metadata from thousands of academic journals to provide search and analytics tools to clients. These data have application in many areas of scholarship, including bibliographies, research on knowledge flow and scholarly communication, and the impact of publications. Recognizing the monetary value that a firm like Elsevier would clearly see in such research analytics, UCLA raised questions about the
appropriate use of such data, and whether any of the value could or should be retained for the benefit of the university or its authors. UCLA faculty questioned the ownership and control of data by or about UCLA and the process by which decisions about it should be made (Borgman, 2014 p. 4).

**UCLA Data Governance Task Force Charge**

Without a way to answer the many questions raised by these situations, the university was in a place similar to that before the Privacy Board was formed, and it followed the same pattern. By 2014, it was clear to IT leadership that the Privacy Board’s (and the university’s) focus on data protection had not kept pace with that of privacy. The Board certainly had not kept pace with the amount of data the university collected, or consistently acknowledged its sensitivity in a comprehensive way. Similar to the way the ITPB recommended a new governance structure to focus on privacy, the Privacy Board recommended that a body be formed to take a closer look at data protection. Executive Vice Chancellor Waugh and Chair of the Academic Senate Reiff formed the ad hoc joint Academic Senate–Administration Data Governance Task Force in August 2014.

The charge letter directed the committee to address concerns over the “ever-expanding amount of data” being generated, captured, and circulated about campus community members. The authors acknowledged that great benefits derived from this collected data, but expressed concern about its potential misuse. The Task Force had two goals: First, to “articulate underlying principles about the use of these data.” Second, to “ensure that we have the capacity through our governance mechanisms to consider campus data holistically and address both current and potential issues” (Waugh & Reiff, 2014 p. 1). Those mechanisms should “address new data requests, resolve conflicts, and align policy and practice among data stewards.” The charge asked the Task Force to consider the intersections of policy and practice, consider models from
comparable institutions, and evaluate whether existing governance structures could sufficiently “address and administer the growing concerns.” If the Task Force recommended a new governance structure, it was to include details about scope and authority, criteria for membership, scalability, and available resources. The group would also need to determine how the governance structure would identify issues and work with the rest of the community. The Task Force could have been named the Data Protection Task Force, but the administration wanted to make it clear that data protection was a subset of data governance and that it needed a broader approach to answer questions about what should be done beyond protecting it.

Observations and Predictions

I am currently the Task Force’s graduate student representative. At the time of this paper, we are nearing our objectives and expect to submit our final report in April 2016. Through my participation, I have made a few relevant observations.

Several themes have been prevalent throughout our discussions. One is the ethical use of institutional data, particularly student data. We felt strongly that we need to govern our own practices, even if the data remain in the institution. We discussed at length how to obtain informed consent when reusing data for anything other than its original purpose. We also agreed that the university must provide a mechanism for individuals to correct or retract information about themselves.

Another common theme has been harm reduction. We understood how valuable our data is to third parties. Members of this group were very concerned about the real cost of exchanging our data sets for "free" analysis. We asked ourselves if there were ways ensure that the people the data are about gain any tangible benefit and if so, does it outweigh potential harm? Even in instances of no clear harm, we raised questions related to the ethics of institutions reaping the benefits of valuable personal data. This was seen as particularly important when students entrust
the institution with their data without necessarily understanding its value. Would they be able to opt-out of learning data collection, for example?

We have also focused on the data itself, discussing ways it should be categorized. In terms of compliance, data used for internal evaluation is the biggest gray area of currently allowable use. But considerable quantities of data can fall into this grey area without the possible implications being fully understood. Without principles and/or a governing body, there is no clear way to distinguish which data could have undesirable or unforeseen consequences. But categorizing data proved to be a stumbling block. The group attempted to begin with use cases and move to categories, but faltered somewhat with that step. Simply comparing and contrasting data sets was a very involved process, and categorizing it proved even more difficult. It was often clear which characteristics certain types of data had in common, but defining them was very time consuming.

Our biggest challenge has been time. Our charge allowed for an 8-month timeline to deliver, but the 11 disparate members could only gather four times in that period, which was enough for productive discussion but not for concrete decisions or statement drafting. This was not a fault in leadership preparation: the co-chairs provided detailed agendas, timelines, and extensive background materials, but the issues and goals would have benefitted from some development and improvements in communication at the outset. Six months after our missed deadline, I spoke with a co-chair who revealed that in that short time, he had managed to distill the concepts further in his own mind and could explain them more effectively. This is an example of how the investment in process discussed earlier in this chapter operates. Being proactive enabled the group to discuss emerging issues and develop principles before any crisis occurred. But that level of proactivity requires navigating new territory. The group had to perform a high level of conceptualization about its own purpose, then create its own categories
and definitions, then decide how to situate the issues in its charge into that foundation. Without a distinct roadmap, these were time-consuming processes, requiring hours of discussion and debate. In light of the Privacy Board’s Privacy Statement precedent, in retrospect, a timeline of less than a year was quite ambitious.

In its forthcoming report, the group does not recommend a new governing body, despite an early desire to do so among some participants. During deliberations, the group considered a body similar to the IRB that would oversee data that fall into the internal “evaluative” gray area. We considered the Privacy Board and IRB as models and were disinclined to recommend a similar standing body. Instead, we will recommend that UCLA extend Privacy Board and the Oversight Committee on Audit, IT Governance, Compliance, and Controls to determine appropriate data use. Additionally, we will recommend that the CPO develop a workflow to receive data governance related inquiries, direct them to the appropriate campus unit or decision-making body.

We will also suggest an awareness campaign to educate state stewards about their responsibilities. The campus can learn from the early Privacy Board struggles to establish itself as a resource, and focus on awareness early in the strategy. A move toward large-scale data governance will impact many academic and administrative groups. I witnessed one example in the Fall 2015 concerning learning analytics. Commercial third parties are not UCLA’s only option; in 2014, UC drafted a pilot proposal to create a shared analytics repository tool, sourced from campus LMSs to gauge interest in third party tools and “explore the effects of technology on pedagogy” (UC Educational Technology Learning Group, 2014). The issue has also been discussed many times by UCLA’s LMS administrators (of which I am one). These efforts are promising, but would benefit greatly from consultation with a data-governance resource before we build or adopt any solutions. Currently, LMS administrators are exploring analytics options
and their compatibility with existing systems. But we will be inclined to make decisions without a truly informed perspective. We plan to consult the Academic Senate subgroup charged with strategizing student assessment in an online learning environment. However, no concrete mechanism is in place to weigh multiple interests and adjudicate conflicts. In a decentralized environment, it can be difficult to even identify all the stakeholders. The issue would benefit greatly from a set of principles or a list of requirements to apply while we evaluate the options.

**Conclusion**

As demonstrated in this case, when academic freedom values are intrinsic to institutional governance, those values are expressed through structures and processes. Through its role in the larger shared governance structure, the Privacy Board has been responsible for preserving the educational mission by establishing principles and actively guiding operations. At UCLA, shared governance has become a value unto itself, not just the practice of values, but an aspirational expression of ideals with both symbolic and functional implications. It represents an ongoing effort to align IT policy with a value-driven mission.

Interviewees were not in complete agreement about how successfully the Board has fulfilled its dual visionary and operational goals. Their opinions were unsurprising, and clearly shaped by their various responsibilities and experiences on campus. Some believed the Board had properly focused on principles and were content to play an advisory role. Others expressed frustration at the Board’s lack of agility and supported a more responsive direction. Either way, however, the Board is fulfilling its mission as it was originally conceived by founders, with wide representation but limited involvement. One interviewee pointed out that, administrators typically brief Board members on issues, either before or after decisions are made, so they are able to share a range of informed perspectives. But no matter the quality of their dialogue, the Board’s influence is mostly indirect. Future IT governance structures should consider the costs
(particularly time) of a large, well-represented standing committee that meets frequently enough to make decisions in the context of its goals.

If the Privacy Board and the Data Governance Task Force are any indication, crafting principles is an arduous process that tends to take more time than expected. If a committee’s charge is visionary and operational, that timeline will stretch further. However, IT committees at UCLA have many overlapping members, people who are accustomed to working together in different contexts. Over time, they have developed a value-based shared language, and now have experience with visionary goals. If harnessed well, they offer an opportunity to build on past lessons, lowering the relative cost and increasing the potential benefits of a new structure.

In the next chapter, I build on the previous two cases to investigate the role of stakeholder relationships in UCLA’s policy. A few themes from this chapter carry forward, including a commitment to principles, shared governance, and cooperation.
CHAPTER 4  
UCLA’S STAKEHOLDER RELATIONSHIPS  
IMPLEMENTING THE DMCA ON CAMPUS  

Overview  

UCLA continuously engages with and negotiates several layers of competing internal and external interests to serve its mission. This case study is about the rise of illegal file-sharing on campus networks starting in the early 2000s, and how the university reacted to legal pressure ranging from legislation to litigation. This chapter discusses how the university honored the institutional values discussed in Chapter 2, namely privacy as related to academic freedom. Reaching back to the roots of the Electronic Communications Policy, UCLA reapplied those core values to other digital content on its networks.  

This chapter also explores the ways the university used IT governance structures discussed in Chapter 3 to maintain a strong and mission-driven position in the clash with entertainment-industry stakeholders over intellectual property. The Privacy Board had an important role in the campus’s response to illegal file-sharing issues, particularly in interpreting values and communicating those values during negotiations with internal and external stakeholders. Again, this case is an example of how privileging academic mission and values above all leads UCLA to take a different approach to policymaking and implementation from other universities. As it had done in other IT policy cases, UCLA decided that file-sharing issues were not merely about technical compliance with the law, but were cultural issues that required a more complex and nuanced approach. In telling this story, I demonstrate how such a contextualization drew from and fed back into the policy context.
The chapter begins with a brief overview of illegal file-sharing practices (also referred to as piracy, peer-to-peer, or P2P) and the DMCA, federal legislation passed to amend copyright law and give greater power to copyright holders to file copyright infringement claims and seek restitution. Following that, I discuss UCLA’s reaction to this law and how it handled legal pressure from digital content producers claiming infringement by UCLA students. My interviews with administrators, IT support staff, and faculty members give insight into the details of how the university reacted to outside stakeholders, and how it formulated a unique strategy to address their concerns while sustaining its own institutional interests. The narrative also draws on documentary sources, including meeting agendas and notes, internal memoranda and training materials, press releases, publications, and presentations. Through the voices of my interviewees and supplementary documentation, I discuss the interests of various stakeholders, how they interacted, and how UCLA formed its strategy. After synthesizing the interviews and documents to trace this story over a decade, I argue that this is a case where a holistic approach was the best way to meet the needs of multiple stakeholders at once, made possible by a unique perspective and multifaceted mission. I conclude the chapter with a discussion of the wide-ranging influence of the holistic approach taken and tested throughout this case and how it has been applied to similar concerns that arose around digital publishing and instructional media.

**Background**

In 1998, the U.S. Congress passed the DMCA to amend U.S. Copyright law. The law had several important, and to a great extent unprecedented, provisions and consequences: (a) criminalizing the circumvention of DRM measures, (b) increasing the penalties for copyright infringement on the Internet, and (c) limiting the liability of Internet service providers (ISPs) in copyright infringement cases. Before the DMCA, Title 17 of the U.S. Code protected the copyrights of digital media content like music and movies, as it had always done with media
content in analog media. Artists and production companies own the rights and, with narrow exceptions, consumers cannot legally produce or distribute copies without permission. The first-sale doctrine limits certain rights of copyright holders, allowing distribution to secondary markets such as library lending, video rentals, second-hand book stores, and the subsequent sale of legally purchased media by individuals (*Copyright Law of the United States*, 1947, sec. 109). For instance, an individual who purchases a musical recording on tape or disk may lend or sell it to another individual without infringing distribution clauses of copyright law. Because physical copies are limited in number, these provisions posed little risk of significantly impacting the primary market for copyrighted works in traditional formats. Digital media, in contrast, can be duplicated and distributed easily, quickly, and in vast quantity, so rights holders of digital content contended that an individual can potentially share a single purchased CD or DVD with enough other individuals to threaten the market. By the mid-1990s, digital-content producers feared profit losses due to a growing illicit market of file trading, particularly music and movies, but also to a smaller extent, other digital content like software, videogames, and books. In this changing technological context, lobbyists for the entertainment industry, particularly the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) pressured Congress to amend existing copyright law to tighten restrictions on secondary distribution.

An explosion of technology enabled secondary distribution in the 1990s. As consumer networking bandwidth increased across the world, desktop hard drives grew and the industry introduced devices like MP3 players and CD/DVD drives that could play home-burned disks. These converging technological advances fostered growth in available software that allowed consumers to copy their purchased disks into compressed digital files and send them across free or low-cost Internet sharing services to anyone around the globe. Initially, media producers
attempted to lock content and thwart copying by building so-called DRM measures that restricted users' access to content, directly into hardware platforms and software code. But these proved cumbersome to legal customers and were largely ineffective against piracy (Sudler, 2013). Facing a world where anyone with consumer-level hardware, home Internet, and minimal technical knowledge could enjoy all their favorite entertainment for free, the entertainment industry panicked. They joined forces and lobbied Congress for additional oversight to criminalize file-sharing behaviors and protect against DRM circumvention, as well as clarifying the liability of ISPs when end users used their networks for illegal file-sharing.

In the early days of the DMCA, the RIAA and MPAA focused much of their collective energy on college students. In some ways, this made sense. By the mid- to late 1990s, the number of students who brought their own computers to college rapidly increased. Many campus residences had high-speed Internet connections and services provided by the institution. College-age students were generally more technically savvy than their older counterparts. They also had lower incomes, but tended to spend larger percentages of their disposable income on entertainment. They were poised to abandon commercial models of consumption in favor of cheaper alternatives.

Higher education institutions entered the fray because the DMCA classified them as ISPs, which under the new law were liable to some extent for content shared illegally across their networks, and thus were entities to whom content creators could serve copyright-infringement notices. However, the DMCA has some liability limitations, granted to ISPs to allow them to “quickly dispose of certain infringement claims without concern for liability to either the infringer or those who claim infringement” (Copyright Law of the United States, 1947, sec. 512).

This safe harbor is available under a few conditions. The ISP cannot have knowledge of infringing activity, or if it becomes aware, it must expeditiously remove the content. It cannot
benefit financially from the infringing activity. It must register a designated agent to receive infringement notices. It must also implement a policy that provides for the termination of services to repeat infringers. Additionally, an ISP must follow procedures to accept notices from claimants, and provide them to alleged infringers. However, the UC guidelines remind the campuses:

The Act does not require a service provider to monitor its service or to seek facts which would indicate infringing activity. Such “policing” activity, in fact, may have the effect of eliminating the liability limitation available under the Act because the provider would no longer be “unaware” of infringing activity—a prerequisite to invoking the liability limitation provided by the DMCA. (UC Office of General Counsel, 1999, p. 5)

Despite the safe-harbor provision, universities faced the challenge of managing content on their quickly growing campus networks, in their dual role as educators and ISPs. This was particularly difficult at UCLA, which had networks already governed by the Electronic Communications Policy. The ECP restricted the type of access copyright holders wanted in order to search for instances of infringement. Citing the ECP, UCLA denied outside access to their networks, choosing to act only as a conduit by matching incoming infringement notices with their end user and passing them along. An interviewee noted that UCLA’s refusal was not alone in this position; commercial providers like Verizon and ATT had also resisted active monitoring at various points to protect their clients. Commercial ISPs had different justifications and varying degrees of success, but they had an active role in how the DMCA and its proponents were viewed outside of higher education as well.

The late 1990s and early 2000s saw a rising tide of increasingly strident and sensational publicity about piracy. Consumer awareness of the issues grew as stories spread about punitive and expensive copyright infringement lawsuits against students and their families, resulting in a backlash against the RIAA. There was a mounting national discussion about the meaning of intellectual property in modern society; critics argued that the DMCA constituted legal
overreach, unduly privileged rights owners, and undermined the consumer, educational, artistic and public information protections enshrined in the original copyright law. But due to copyright law’s complexity and the challenges created by new technology, the DMCA fed the proliferation of misinformation, fear, and confusion.

**Stakeholders**

This story involves UCLA’s multiple internal and external stakeholders and their different values and missions. The major external players were entertainment industry groups such as the MPAA and RIAA, and the studios and other content producers they represented. Congress had a critical stake in deciding how to write legislation that would respond to industry interests and the pushback from consumers, ISPs, and institutions. After the law was passed, lawmakers had an ongoing role in assessing the responsibility of universities to curb illegal file-sharing on their campuses. Universities had a stake in protecting themselves as well, and the differences in their responses continue to highlight how the policy context affects decision making.

Internally, the DMCA legislation affected large parts of the UCLA community, particularly UCLA’s legal counsel, Student Life offices, IT support, instructors, researchers, and students in residence. Several units on campus were involved with modeling UCLA’s response to the DMCA and continued to have ongoing roles in enforcing it, including administrative offices like Housing and Hospitality Services, Information Technology Services, and Campus Counsel. External Affairs offices involved include Federal Relations, Media Relations, and State Relations. In Student Affairs, the Office of the Dean of Students, Office of Residential Life, Orientation, Student and Campus Life, and Student Legal Services all lent their expertise to the issues. UCLA Policy 464, *Online Copyright Infringement Liability Limitation*, names those responsible for determining whether infringers should be subject to a restriction of access to
campus IT services. They are the Vice Chancellor for academic personnel and staff, Deans for faculty, and the Dean of Students for students.

The majority of this case study focuses on students in campus residence, but copyright law and campus policies are also an important part of research and instruction, particularly because several copyright exceptions apply to schools and libraries. The campus directed a majority of its piracy-related efforts at students, but policies apply across the UCLA community, and are an important part of the story.

**UCLA Fields Infringement Claims**

**Policy 464**

UCLA Policy 464, *Online Copyright Infringement Liability Notification*, which went into effect August 1, 2000, was written to address DMCA requirements. It establishes the university as an online service provider, and details the requirements that must be met for safe harbor to apply. The university defined Online Service Provider to refer to parts of the institution as well as the whole. The policy applies to “the individual campus units or departments that provide online access services to the UCLA community including, but not limited to, schools, divisions, departments, libraries, and labs.” It states that when a UCLA faculty member, staff, or student receives a copyright-infringement claim, designated campus officials “shall respond to evaluate the basis for the allegation and will take action, as warranted, to end the infringement in accordance with existing UC policies.” It will also pass along to the infringer any financial liability that the university incurs on their behalf. Policy 464 further defines the duties of the designated agent. The agent is required to follow the terms in the DMCA, but at UCLA is also responsible for “making the initial determination as to which campus units, departments and Online Service Providers are involved and notifying the Vice Chancellor—Legal Affairs.” Then,
the appropriate administrator determines the infringement penalty comprising a restriction of access to campus technology services. The Vice Chancellor for Academic Personnel and the deans are responsible for faculty; the Dean of Students oversees students who were not acting in their capacity as a UCLA employee; the appropriate Dean, Vice Chancellor, or Vice Chancellor of the Medical center, for staff. Administrators decide invocation of the Liability Shelter on a case-by-case basis, being “mindful of issues of academic freedom and the research and instructional responsibilities of faculty and of existing defenses afforded by, for example, the fair use provisions of United States copyright law.”

An Infringement Notice Influx

Around 2002, UCLA experienced a sharp increase in the infringement notices it was receiving, mostly from the RIAA. Initially, infringement notices were poorly issued—they were in hard copy and not always addressed to the campus DMCA agent. The RIAA was also making mistakes, sending notices with inaccurate claims, which allowed the university to simply return them. But it was a slow manual process of mailing claims on paper.

At that point, UCLA would forward the notices to the student and advise them to pay fines or seek legal counsel, but did not take action beyond that. In particular, administrators would not release any names or other identifying information associated with the IP address in question, or intervene further in the process. The university maintained this one-way flow of information, much to RIAA’s consternation. Once the campus DMCA agent received the notice, the agent would forward it to the student, along with directions to address it with their Dean, and withdrew without any legal intervention. From there, the student chose whether to file an objection or take other legal action.

Met with what it regarded as resistance, the RIAA took two other approaches. The first was to establish a more aggressive stance by issuing subpoenas for infringing IP addresses;
RIAA sued a few students with this approach. The second tactic was to attempt drawn-out lawsuits by sending UCLA’s agent notices with directions to pass them along to the student suspected of infringement with an offer to settle for $500.

And they started sending notices, which is not consistent with the DMCA; it’s not technically something that we had to pass on to the students. So the DMCA agent getting these letters saying notify student at this IP address that they can settle this case by going to this page and clicking. And you go to the page and it looks like you are admitting that you are a horrible criminal offender and you pay your money and you’ll be on your way.

I remember there was an initial flurry of course, of students freaking out saying, “OK I got a notice and I did what you told me to do and now they’re sending me this settlement thing so what am I supposed to do?” And so we had actually the student legal services provide help to students who either wanted to settle and get out of it and that was kind of a real big flurry of activity, and I think that really dropped off. There may have been a handful of students who paid some, a minimal amount, to settle, all on an individual basis. We didn’t hear about it because it was their private legal matter but it really caused a big debate as to what our role should be in passing along these settlement notices.

Infringement notices again increased in 2007 and 2008, a result of RIAA’s new strategy. In February and March of 2007, RIAA industry officials issued universities hundreds of pre-litigation settlement notices, approximately 30 of which went to UCLA, to be forwarded to the infringing users, offering them a discounted rate to avoid a lawsuit. Unlike notices in the past, which included the date of the infringement, the filename, and the software used, these only referenced the IP address, leaving responsibility to the university to alert the user about a pending lawsuit (Truong, 2007, para. 11).

The Spring 2008 issue of In Focus: The UCLA Student, a magazine circulated to students, featured an article about file-sharing at the university. Spurred by the pre-litigation letters, the article provided warning and reminded students about legal alternatives.

During the academic year of 2006–2007, UCLA received 59 pre-litigation letters for students from the RIAA along with a number of demands for identification of student copyright violators, a move that immediately precedes alleged offenders being sued. … Since 2005, fewer than 10 UCLA students have been sued. (Wyer, 2008, p. 4)
Standing Up to Industry Stakeholders

A mix of stakeholder relationships contributed to UCLA’s high-profile involvement in campus privacy issues. UCLA students may have participated in illegal file-sharing at a higher rate than students at other higher education institutions due to high student enrollment and available technology. A few interviewees remarked that UCLA received more infringement notices than any other university. This is not accurate, though the university was typically among the top 10 American universities with the highest number of infringement notices; in 2007, the MPAA ranked it number four in the country (Read, 2007, para. 5). But the widespread notion that UCLA was consistently highest demonstrates a pervasive sense on campus that UCLA drew a disproportionate amount of attention from the government and the entertainment industry, due to their influence locally and in the state more widely.

UCLA’s Hollywood Connections

There does appear to be some truth to the common perception that UCLA has a unique relationship with the entertainment industry; a relationship that had a significant role in copyright-infringement arguments. I asked each interview participant in this project about this possible connection and all indicated they recognized the phenomenon, and gave their opinions about contributing factors. One interviewee had heard about it from colleagues:

I’m a believer, only because people have told me that [UCLA has a relationship with the industry] ever since I stepped foot here, that we’re right in Hollywood, we’re right here and its easy for them to come after us, and its easier for us to work with them. I mean, [Vice Provost James Davis] has relationships with all kinds of people in the industry and we’ve had people here from the different studios to come and talk to us, and it’s really easy for us to get together.

The respondent suggested UCLA and the entertainment industry are the biggest employers in Los Angeles, and possibly “feel an obligation to the same community.” The participant was not positive that the significance of the relationship is real, but that colleagues
seemed convinced. The most-cited reason for the relationship was proximity; as one interviewee put it, “Hollywood is just down the street.” Another interviewee agreed, but pointed out that the University of Southern California, although also located in Los Angeles, did not receive the same attention.

You know, we’re right here in Hollywood; we’re an easy target. You know, they can’t just drive across town to harass a private university. I doubt they harass USC anywhere near as much as they harass us. It’s just easier to pick on a public university. And in fact, we’ve had so many encounters with them, we said hey look you know as well as we do that the University file-sharing is about 1% of your problem and the bit torrent and the offshore stuff is 99% of the problem, why are you taking so much of our time and your time when you know the problem is elsewhere? [A studio representative replied,] “well, we can’t get to them.” To our faces! “We can get to you.”

It is likely that as a public institution with reliance on state funding and subject to transparency requirements, studios believed the university would be subject to additional pressure from the government and thus more likely to capitulate to a revenue-generating industry. Interviewees also pointed out some crossover personnel in the entertainment industry and the UC. For example, Sherry Lansing, former CEO of Paramount Pictures, serves on the UC’s Board of Regents. The state also has a history of industry crossover into politics, including Howard Berman, a California Congressman who strongly supported copyright interests against piracy. Interviewees also noted that record labels and studios tended to have high proportions of UCLA alumni, creating, as described by an interviewee, a “real symbiotic relationship” that is fed into by both proximity and people.

I don’t want to speculate how deep that relationship goes, but I do think that it does affect how we are reviewed and opinionated … opinions by others. Are we a friend? Are we a foe? Are we a partner? Just for my limited experience with these companies, they would come to us first before they would go to USC, before they go to Pepperdine.

The ambiguous nature of this relationship is apparent in many aspects of the DMCA issue. UCLA may have earned a reputation for being proactive and collaborative, but the campus
did not ever cede much ground, opting instead to push back while citing its institutional values and educational mission.

**Attempts at Cooperation**

UCLA participated in several collaborative attempts with film and television studios that wanted to take action, legally and technologically, that were contrary to several institutional values. The university did not accept any RIAA or MPAAAs approaches without debate, nor did the studios back down. The two sides did manage to collaborate and agree on a few important aspects of the problem, but it was not without ongoing struggle.

Well, we totally disagree over pretty much everything, right? So when you get us in the room, we don’t agree, but because of who we are, we collaborate on everything. You have to get everybody’s input, right, from the hundreds of thousands of UCLA faculty and staff before you can do anything, you have to collaborate. That’s what we do. And no one was going to shove anything on us and we weren’t going to shove it on anyone else because that’s not who we are. We always collaborate, you know, come on over, that’s fine, we’ll sit down with the execs from NBC, whoever wants to talk to us. You have a good idea, lets see what we can do. And it was really hard because where they were coming from and what they wanted to do wasn’t consistent with what our mission was from an educational point of view. And from a use of content. You know, we respect copyright, but we’re an educational and research institution, so we have a lot of exemptions that apply, so we are all about access to content and they’re all about shutting down content so when you look at it like that, its like we’re starting from opposite corners and the question is how do you get to the middle.

From the industry’s somewhat paternalistic perspective, higher education students were among the worst infringers and most lived on university property and used university resources, so their universities had a responsibility to curb illegal file-sharing. No one sued UCLA over infringement, but studios did seek administrators for support. To demonstrate that UC and UCLA took copyright infringement seriously, they formed a UC–studios working group with “a core group of MPAA member studios and the MPAA itself in the Los Angeles area.” In testimony at the U.S. House of Representatives, Vice Provost Jim Davis explained one successful result from that group.
The genesis of the UCLA Quarantine approach arose from an early dialogue with Universal Studios and Universal Music Group. At the time, UCLA was articulating what it wanted to achieve and Universal was developing the Automated Copyright Notification System, or ACNS. We proceeded with the implementation of the UCLA Quarantine approach inspired by a number of the concepts in the ACNS framework. (Davis, 2004 p. 2)

The Quarantine approach (discussed in detail later in this chapter) was the first step in UCLA’s copyright-infringement strategy and remains in effect. Automation was key to streamlining the process for sending and receiving notices, as well for involving the appropriate people and responding. UCLA’s Executive Vice Chancellor attributed the group’s success to communication, reporting that “[we] are currently sharing information on illegal file-sharing trends and indicators, discussing policy recommendations to the State Government and considering selective evaluation projects and pilots” (Davis, 2004 p. 6). UCLA’s quarantine approach was a compromise: the university refused to adopt Automated Copyright Notice System, as developed by Universal Studios, but used its framework to develop a version better suited to the university’s mission.

The quarantine approach was a compromise. Before UCLA adopted an automated system and developed the rest of its illegal-file-sharing strategy, the RIAA wanted to install the monitoring software, Audio Magic, on UCLA’s network to track P2P activity. The university emphatically refused, citing the anti-monitoring stance on the ECP. It objected in particular to the type of deep packet inspection that would be conducted by Audio Magic, which did not merely look at connections, but at what was actually transferred. UCLA did not intend to do its own content monitoring, much less allow that much access to a third party.

Inside and outside higher education, the RIAA earned a reputation for its very aggressive tactics. Recalling this, one interviewee called it “the junkyard dog of copyright protection.”
Despite its tenacity, the RIAA had limited success. In the mid- to late 2000s when file-sharing expanded to include movies and TV shows, the MPAA chose a different path.

And then the MPAA, right, totally different. So the RIAA was just in our face, you know, trying to beat on the students and they really didn’t get very far. We put all our systems in place and we educated our students and the MPAA didn’t do that. They sent some notices, but not a lot, and they didn’t do these settlements. They came over and they wanted to talk to us and they wanted to figure out a way that we could collaborate.

During those collaborative efforts, both sides began to advocate their positions in greater detail.

**Institutional Research as a Stakeholder Bridge**

In 2008, the MPAA and UCLA’s OIT cosponsored a field study to be conducted by a group of six students from UCLA’s Anderson School of Management. The team, called Insight Consulting, studied the issue and gathered perspectives from higher education and entertainment-industry personnel. Their goal was to examine potential new business, delivery, and consumer models for digital entertainment. Insight Consulting’s main research question was, “How should a new digital entertainment service be crafted and deployed that most college consumers will find more compelling than piracy?” In March 2008, the Privacy Board invited Insight Consulting and representatives from the MPAA to a meeting for an update (UCLA Advisory Board on Privacy and Data Protection, 2008). Presenters summarized both sides’ positions, and determined common goals and conflicts in hopes of finding solutions that would benefit producers and consumers. They reported that studio representatives had communicated frustration with the perceived lack of responsibility on the part of universities. They blamed universities for providing fast network connections, but skirting the responsibility of policing content. Studios also complained that universities operate under Safe-harbor provisions but do not use the monitoring tools available to them. They discussed several aspects of the issue with the Privacy Board, including the division of responsibility for intellectual-property awareness, piracy.
enforcement, and students’ privacy expectations (Fields, Finley, Leung, Mei, & Raymond, 2008).

The Privacy Board discussion is an example of a strength of UCLA’s governance structure: MPAA representatives were accustomed to addressing administrators, and the faculty members of the Privacy Board were able to take a different tactic to advocate their cause. An interviewee recalled,

We had faculty at the tables because the administrative people from MPAA and the RIAA … they thought they could beat down the administrative people because it’s their job and they had to do it. Where, when the faculty came in and said over my dead body, they were hearing a different voice. A principled voice. So I think that [Vice Provost Jim Davis] and [Chief Privacy Officer Kent Wada] probably had to get bogged down in operational and legalistic ECP type language. And the faculty could come in with a principled argument and say—these are there for this reason.

The meeting also did foster some discussion of the MPAA’s request for the UC to amend the ECP to allow content monitoring. UCLA faculty and administrators were able to present a united front for their campus and the rest of the system with a strong refusal, but one that was methodical. An interviewee remarked that the university was using the ECP as its “big stick” to beat back the incursion, but that the Board was in a good position to explain the reasoning behind it. To do so, Board members and guests discussed what policy changes would be required, what the changes would mean for the rest of the policy and other technologies governed by it, how the community would view changes, and other broad implications. UCLA still has not changed the ECP to allow active monitoring, and by maintaining the holistic strategy discussed in this chapter, is unlikely to ever do so.
UCLA Builds a Holistic Strategy

Testifying Before Legislative Stakeholders

In 2005 and again in 2007, UCLA’s Associate Vice Chancellor Davis provided testimony to the U.S. House of Representatives Subcommittee on Courts, the Internet, and Intellectual Property. At these hearings, Davis established UCLA’s intellectual-property respectful position, as a creator itself. Davis reported on UCLA’s strategy to curb piracy on campus networks, explaining the reasoning underlying the university’s decision to address illegal file-sharing as a student-life issue, rather than a technological issue.

At the first hearing, Davis explained the UCLA quarantine approach and shared promising preliminary results; however, Davis also stressed it was defensive solution, one that is only “reactive to notifications of infringement,” and that UCLA sought a “multifaceted strategy” with other measures to compliment the quarantine. One was a branded outreach program across UC campuses. The UC would issue a request for proposals with the goal of “facilitating access for UC campuses to legal on-line entertainment media services” providing music and movies to meet a growing demand.

Davis followed up on the strategy at the second hearing, presenting the university’s commitment to finding a sustainable solution that would amount to more than a short-term solution by integrating the issue into the campus culture:

We are looking at infringement cases in a more holistic sense judicially as well. A student may demonstrate patterns of behavior that indicate a need for help, and treating illegal file-sharing as a separate issue is not always in the best interests of these students. By reviewing their behaviors holistically, we can help them identify underlying causes so they can make changes and continue to thrive academically. (Jim Davis, 2007, p. 36)

Davis outlined the three-faceted strategy that UCLA had developed and tested in the intervening years: (a) quarantine by automated technology, (b) a proactive effort to offer/encourage legal
activities, and (c) an integrated educational campaign. Each piece of the strategy was essential to comply with the law while maintaining the university’s values and mission.

**DMCA Strategy Step 1: Quarantine**

The first step, quarantine by automated technology, went into effect in Spring 2004. The goal of the UCLA quarantine approach was an automated system to quickly and automatically route copyright-infringement claims to the alleged offender, with the first offense treated as a teachable moment. By framing infringement as a teachable moment, the university established the need for proper education about intellectual property and its intersection with education.

A letter to the UCLA community and an article in the *Daily Bruin* summarized the four-step quarantine process. First, the copyright holder notifies the university, supplying the offending IP address. If that address corresponds to UCLA housing, it is mapped to the machine’s media access control address and its owner. The university restricts the identified computer from full network access, and limits it to a few local UCLA domains including the Library, course websites, and Student-Records systems. Additionally, the Judicial Affairs Coordinator and the Assistant Dean of Students generate an e-mail to the student, providing notification of the claim and quarantine, directions to remove the illegal content, and directions to accept the acceptable use agreement. A first-time offender must only acknowledge the notice, which is not an admission of guilt (Hodge, 2004; Naples & Davis, 2005). As Davis pointed out in both Congressional testimonies, the quarantine is the first step in shifting a copyright-infringement notice from a strictly legal matter to a campus judicial matter. It also streamlines the process and keeps attention on due process and education, where it is most critical.
Notification and Acknowledgement

The university carefully crafted the notification process so as to not imply that acknowledging the notice was an admission of guilt. Students only had to acknowledge that they were aware of the facts, that they had reviewed the appropriate-use policy, and agreed to adhere to it. The university also informed the student that, if the notice was accurate, they understood they were to cease sharing copyrighted content. The university did not expect students to stop using the software altogether, or remove it from their computers.

At the time, many higher education institutions were mandating removal of P2P software on student computers, but UCLA took a hard stance against that on the basis of academic freedom. UCLA would provide technical support if the student wanted to disable or remove the software, but did not require that action. The university wanted students to recognize that simply running the software was not illegal, only the infringing behavior was. Furthermore, intellectual freedom necessitates access to information, and peer-to-peer platforms provided that. Although students rarely used the software for legal purposes, UCLA did not consider this a strong enough reason for a ban. The university wanted to be clear about the difference between the value-neutral nature of the technology itself, and its various uses. As with other academic policymaking examined in this study, context mattered. The university also saw an opportunity for students to gain a greater awareness of what software their computers were running, how to manage it, and how to distinguish between acceptable and unacceptable uses.

Among interviewees, accounts of how the right to keep file-sharing software was communicated to students varied slightly. Some recalled that the policy did not ask students to remove the software at all; some indicated they did ask for removal unless the student provided a valid reason for continued use. Either way, the university did give students some discretion, while also providing technical support:
A lot of times the students wouldn’t even really know that they had the software, that it was put on your computer when you downloaded a file, or how to turn it off so we would have them go to the computer lab who would help them take it off their computer. But we didn’t want to mandate that they remove it because there’s legitimate research and education purposes that you might want to have file-sharing software on there so our debate was really that it’s not the technology that’s bad. It’s not bad technology, it’s education about using it.

UCLA’s IT support staff believed it important to teach students about how their computers interfaced with the network and how to configure them in the most secure way. However, when a security expert began advising students, others objected:

And I argued, this is a security problem. I need to inform the public. And they would come and say well you’re telling kids how to download stuff without getting caught. And it’s like, no, this is a security issue. I need to tell them how to configure LimeWire so they’re not sharing their desktop.

**Proposed Quarantine Software**

Some IT support staff wanted to provide more tools for students to assess their networking behaviors. In 2007, a staff member brought to the Privacy Board a piece of software called Be Aware You’re Uploading (BAYU) created by the University of Michigan. BAYU watches for computers to establish peer-to-peer connections and sends an e-mail to the user asking if they are aware of the outbound connection. The Office of Student Affairs was interested in this method because administrators recognized the possibility that students’ computers could be infected with malware that was establishing P2P connections without their knowledge. Student Affairs staff brought this idea to the Privacy Board, arguing that BAYU only used automated monitoring that investigated transmission, not content. Student Affairs staff argued that the benefit would outweigh the privacy risk. Their notice to the privacy board asserted

BAYU would be a welcome and complementary component of UCLA’s comprehensive student life approach to addressing illegal file-sharing … BAYU is an educational tool to help students, but it is also a technology-based tool that could satisfy proposed Federal
legislation to require that such tools be deployed (especially if BAYU becomes widely adopted). (UCLA Advisory Board on Privacy and Data Protection, 2007, p. 2, see Appendix E)

An interviewee recalled the thought process behind recommending the adoption of BAYU in the interest of warning students who were running P2P software:

All of our infringement notices that were coming from the entertainment industry were from downloading through the use of these peer-to-peer file-sharing programs. So, it was like, why not make it opt-in? We are not banishing it. When I say to graduate students that they can’t use it, or researchers can use it. I’ve yet to see an undergraduate who had a reason to use P2P for work. … I just thought that would’ve been a good idea.

BAYU’s supporters saw value in an opt-in program for students to assess their own computers’ traffic and have the option to ask technical support staff to remove P2P software. Several aspects of BAYU seemed like a good fit. The opt-in aspect was most important—with an automated system, only the student would know if his or her computer was identified, and could choose whether to take action. BAYU did not directly compromise the ECP or conflict with security standards. The Privacy Board was not convinced; BAYU did not fit their definition of “privacy respectful.” Board members warned against the possible chilling effect any additional monitoring could have. Although P2P software was very rarely used for legal and academic purposes, Board members did not like the idea of the university watching potentially legitimate traffic and potentially stifling students’ intellectual freedom. They also expressed concerns about the ease of expanding the monitoring parameters beyond those initially intended. The possibility of a slippery slope and the potential for misuse were at issue.

After discussion, the Privacy Board advised against implementing the software, advice that was not binding but had enough weight to dissuade BAYU’s supporters. A faculty interviewee recalled part of what informed their recommendation: a desire to treat students’ academic freedom with the same respect it does for that of faculty. Some discussion ensued about the danger of prohibiting any particular technology simply because it could be used
illegally. Most Board members agreed with the idea that technology itself is value-neutral, rather than inherently dangerous. In fact, in the interest of academic freedom and access to educational materials, even students who had received an infringement notice were not compelled to remove file-sharing software. An IT specialist interviewee was initially surprised by the repudiation:

My perspective is that I want to keep students safe but really it was the wrong thing to do now that I think about it. But, really I’m glad that Board was there. Because I think that would have been a big mistake for us for us to do that.

By including the Privacy Board in this decision, UCLA’s technical support staff were compelled to see a different side of the argument, again stressing the importance of the shared-governance model. Even with good intentions, a seemingly innocuous piece of software can have wide-ranging academic implications. By having a governance structure in place to inform from several perspectives, those implications could come to light before implementation. An interviewee recalled the experience of going before the Board:

And I never really thought about it—another perception of what it is that we are promoting in preventing. It was really kind of an eye-opener for me and I’m definitely gun shy about ever going back, but I thought their arguments were really well thought out and presented in no uncertain terms.

The quarantine was an important step, but it was defensive and the university knew it needed to discourage piracy prior to infringement.

**DMCA Strategy Step 2: Offering Legal Alternatives**

The second step to UCLA’s holistic approach was to encourage legal alternatives to illegal file-sharing. This was an interesting part of the solution because it meant UCLA was actively involved in choosing, testing, and providing feedback regarding alternative business models for an industry intent on suing its students.

The historical model didn’t fit in the digital age so they needed to come into the 21st century and figure out, you know, how do you provide, digital content, and I think, even
to this day, they still haven’t quite figured it out. And so there’s been discussion from the very beginning, until now, about what is the appropriate business model that will give them what they need to make in order to continue to create content, and will be at a price point that students are going to pay it.

Content creators and owners were slow to make changes, and the university feeling compelled to incorporate this step into their process provided value to the industry with a focused demographic. But UCLA understood this process was an important demonstration of its good-faith effort. Initially, the degree to which the university was involved was not well established. Some arguments emerged about the appropriateness of using university resources to subsidize entertainment. The campus did contract with three different media providers—CDigix, iTunes, and Mindawn—which differed from each other in small ways but primarily offered licensed music downloads at reduced cost. To meet the demand for television and movies, UCLA formed a partnership with iClicker to pilot a university-branded platform, pulling free legal content from different places with a few additional tools like the ability to see what people on campus were watching. The iClicker partnership was not popular and was not pursued.

After a few years of lackluster results, the university let its contracts expire, realizing that, as one interviewee explained: “There really wasn’t any economic solution that worked for the university that the students would have accepted.” Instead, Student Affairs opted to concentrate resources on Step 3 of the strategy: outreach and education.

**DMCA Strategy Step 3: Educational Outreach**

The third step in UCLA’s strategy is the keystone of the holistic approach, and one that, in tandem with the quarantine, set it apart from other institutions. As it did with information-privacy issues, UCLA acknowledged that piracy on campus was a social as well as technological issue. The outreach and education elements of the strategy directly reflect the desire to integrate these issues into student life.
Details of the outreach and education components have changed over time. Outreach efforts steadily expanded from 2004 to 2012 to include branded informational campaigns, print materials, websites, videos, and presentations. During that same time, the UCLA strengthened its training resources along with its sanctions. Initially, in 2004, first-time offenders only acknowledged the claim and delete the offending material. The Dean of Students summoned repeat offenders, with punishment varying from warnings to suspension. By 2007, however, the university directed first-time offenders to online training and asked them to reaffirm their agreement to follow the student code of conduct. Second-time offenders had to write a paper and attend an ethics workshop. A third offence subjected students to a year of academic probation or suspension. After administrators observed a rise in recidivism in 2008, the university required educational workshops for first-time offenses, and sent repeat offenders directly to the Dean of Students for academic probation or suspension.

Outreach

UCLA employed (and still employs) several tactics to reach students with information about the risks of illegal file-sharing. The university introduces incoming students to file-sharing rules and procedures during orientation. Before they move into the residence halls, students must sign an In-Room Computing Acceptable Use Policy as part of their Housing Contract. The Office of Student Affairs circulates fliers and makes presentations to several student groups throughout the year.

Student Affairs also initiated the “Think Twice” campaign in 2013, informing students of the number of infringement claims received for computers on their floor, in an attempt to bring the likelihood of getting caught closer to home. An IT-support interviewee recalled this policy as a particularly effective way to get students’ attention. Video monitors in residential halls, the recreation center, and Residential Life offices displayed in real time the numbers of students
caught sharing illegally. Another interviewee recalled one “couldn’t get onto an elevator without seeing one of those things.” However, despite its visibility, the method was unsustainable. It became too time consuming for staff to receive infringement statistics and communicate them to resident assistants in time for them to be effective. Additionally, the method backfired in a few of the smaller residence halls; if a floor received zero notices, its students were much less likely to take the risk seriously. After two quarters, the campaign ended.

The university created several websites for outreach, some of which are still maintained. In 2008, the Office of Intellectual Property and Industry Sponsored Research published a website sharing general information about intellectual property. The 2008 (updated in 2012) “Get Legal” campaign hosted a site which, along with facts and explanations, maintained a list of legal online content including TV, movies, music, and some online vendors. These websites aimed to settle some confusion of what was and was not legal to share, and why (UCLA, 2012). To many students, it was unclear why they could watch episodes of TV shows on a free streaming service like Hulu, but not access those same episodes using P2P software.

**Workshops**

The other essential piece of UCLA’s educational strategy was for the Office of Residential Life to build specialized training workshops, lead by the Dean of Students Ken Heller. These workshops ran several times per quarter, were mandatory for offenders, but were also open to any interested students. Mandatory workshops had a completion deadline to qualify for certification, a method of discipline similar to other violations of the student conduct code, another way this approach is integrated into the student life experience (UCLA, 2012, p. 3).

Several interviewees credited the success of the peer-to-peer workshops to the Dean of Students, Ken Heller, who insisted on the responsibility to interact in a meaningful way with students. Heller explained,
You know, we created this mechanism and I was the front guy. Because I was the one who had to also receive the unhappy communications from students—‘how dare you; you’re wrong; what you mean by that?’ You guys are just … you’re out … you’re working for … the company.

Perhaps not surprisingly considering the UCLA culture, Heller took an academic approach to work by leveraging knowledge of behavior and psychology. Heller began to offer workshops weekly to shorten the gap between bad acts and intervention. Workshops covered all aspects of file-sharing and legal alternatives. Beyond that, Heller took responsibility for a vast majority of the university’s educational outreach by managing all residential DMCA cases. In the workshops, Heller explained infringement, how copyright holders found infringing behavior, and how the university identified an IP address and matched it to a computer. Heller found that the most effective workshop format is informal discussion.

We start out by asking people, so what you get busted for? And already know what the answers are. “So how many people for movies? Would you get? Would you recognize it?” And they’ll laugh, and I’ll say, “Well, you might as well get something out of this.”

According to an interviewee, approximately 90% of students admit to the infringing activity in this environment.

Heller framed the discussion much like the university did in its formal responses to industry and government inquiry—by positioning UCLA as a creator of intellectual property. He explained to students that beyond education, UCLA is “in the intellectual property business” and students themselves are creating protected works, thereby engaging them on a personal level and showing them their stake in the issue. Heller also offered explanations about the differences between P2P file-sharing, paid downloading services for music and movies, and free and paid audio and video-streaming platforms. Overall, the Dean tried to impart a wider view to students about how getting caught can have long-term consequences to their academic careers and future employment.
Balancing Multiple Stakeholder Interests

A Holistic Approach to Multiple Interests

When digital-content creators and producers began pressuring UCLA to take responsibility for illegal file-sharing on campus, UCLA faced multiple competing interests. In response, the university turned inward first, in an attempt to establish a strong and cohesive position that could stand up to legal claims against the community. Administrators turned to existing policy like the ECP to legitimize its anti-monitoring stance. They also used the university’s mission to solidify its role as an institution that educates students in and out of the classroom. Administrators were able to rely on the existing governance structure for several aspects of their strategy, thereby engaging the entire campus community. By creating a robust set of policies to address illegal file-sharing, the university could remain in compliance with the law, stand against external interests that conflicted with its values, and leverage its considerable size and strength to establish itself as a leader in higher education.

An IT staff interviewee credited UCLA’s administration for not making unilateral decisions on this issue, but meeting with all stakeholders to collaborate. An interviewee summed up the buy-in process as “frustrating but also great,” a sentiment shared by all of the interviewees at some point. Repeatedly, interviewees described UCLA’s inclusive decision making as irritating, but ultimately worth the effort. The results were especially important in this case, because in the face of immense external pressure, the university gathered the strength to defend itself by implementing a strategy in which faculty, administrators, and IT employees contributed to various pieces of a social/technological issue.

Other interviewees remarked on the synergy inherent in the roles of those with piracy-related responsibilities: strategy, policy, operations, and as one called, it the “where the rubber meets the road” discipline. Though it is a large university, those with technology-related
positions have had relatively long careers at UCLA and work together regularly. Whether or not they agree with every step, the interviewees in this project (and in my experience) vocalized support for university strategy and acknowledged it the most effective way to make and implement appropriate IT policy.

**Recognizing a Technology Issue as a Societal Issue**

By reframing a technological and legal issue as a social and cultural issue, UCLA could protect itself and its students while using valuable teachable moments to educate the campus community about digital citizenship. Consistent attention to academic freedom values ensured students did not lose access to their instructional materials as a result of infringement claims, nor were they punished in ways inconsistent with their code of conduct. By framing illegal file-sharing as a cultural issue, university administrators could maintain the concept of technology as value-neutral, and differentiate the technology itself from its right and wrong uses. By choosing a holistic approach, the university could meet the many related concerns arising from a single technological issue.

As in the other cases, illegal file-sharing was initially considered only a matter of compliance. In response to the legislation and pressure from outside stakeholders, the university designated an agent to receive infringement notices, and built an automated system to notify users of complaints. After establishing those basic procedures to meet legal requirements, the university decided to leverage its institutional influence as a gatekeeper. This allowed UCLA to meet ECP guidelines by protecting its network and community from content providers’ reach. It also meant the university could actively engage students rather than acting as a passive notification conduit. This comprehensive approach aligns with UCLA’s institutional culture, which often attempts to manage internal and external stakeholders with the same actions.
Societal Good and Citizen Building

As in the other cases, the point at which UCLA’s policy deviates from other universities is in service of an institutional value and the university mission; in this case, academic freedom and citizen-building. UCLA’s strategy included a quarantine method that did not interfere with a student’s education by allowing online access to essential campus services during impending infringement claims. By not monitoring traffic or requiring the removal of P2P software, the university preserved essential elements of privacy and free inquiry. By eschewing a punishment model and making a long-term investment in behavioral change and ethics, the campus met its mission to educate outside the classroom, promote engagement in campus life, and serve society by teaching students a “renewable set of skills and commitment to social engagement” (UCLA, n.d.). In 2007 testimony, Davis referred to the “obligation to help prepare our students for their lives beyond their years here and to encourage the core values and ethics that will help them to be successful and responsible contributors to society” The university was proud of resisting the impulse to react with a “short-term, defensive or technological solution” in favor of finding that teachable moment they feel necessary to affect sustainable changes in behavior. (Jim Davis, 2007, pp. 1, 9) An interviewee elaborated on the philosophy:

The goal is not to punish. If you talk to anyone on the Student Affairs side, it’s not to punish somebody, it’s to teach them. A lot of times it is a punishment, right? You’re suspended and that’s pretty bad. But really, the idea is not that we’re trying to impose a legal punishment on them, but we’re trying to teach that their behavior was unacceptable so that they can change and hopefully be good citizens when they leave.

The Senior Associate Dean and the Assistant Vice Chancellor examined the student-conduct code and decided that piracy was a type of cheating and a type of computer misuse; two behaviors that were already governed. Rather than creating a new type of discipline, they fell back on existing policy governing student behavior.
UCLA as a Teacher and Leader

UCLA asserts itself as a leader in developing technology but also in its application. The university recognizes its particular mission, which may not align with other institutions, but advocates its position: one that is ultimately in service of academic freedom, particularly including privacy and free inquiry. As Davis stated in this testimony:

Our mission is not shared by organizations outside of the educational realm, so we recognize that short-term measures may be appropriate in other circumstances, particularly when the piracy problem is largely beyond the purview of educational institutions. But at UCLA, we are encouraged by what we have seen and continue to be enthusiastic about the student life focus. (Jim Davis, 2007, p. 9)

An interviewee recalled a shift in personal perceptions to serve the mission.

And it has really changed my view on this whole thing that I’ve been involved in. I thought in the beginning, flat out, that we need to stop this. That’s my job. To prevent it. If we can stop it from the beginning, that’s our job. Well, no, even if we had the power to do that, the more I think about it and more I talk to students, it’s like they have no appreciation for IP. In fact, they have very little appreciation for a lot of things. But they have their perception of it.

Throughout the course of DMCA-related issues on campus, the university has taken defensive and offensive positions. By using a value-driven holistic approach that has become a hallmark, the university was able to reject accusations that higher education was not doing enough to curb illegal file-sharing. As a result, UCLA ventured beyond self-advocacy to stand for higher education in general. UCLA positioned itself as a leader with the creation of the ECP and the Privacy Board, but its reach extended far further in this case. UCLA’s testimony at the U.S. House of Representatives brought national attention. Additionally, the university participated in a wider cultural dialogue as well, sharing its position and strategy in conferences and higher education journals (Wada, 2008a, 2008b).
Looking Forward—DMCA Strategy Reapplied

The entertainment industry brandished their viewpoint internationally, but was not the only industry with business models greatly affected by the demand for new methods of consumption. Academic publishers and providers of academic multimedia also struggled to stay relevant during a push toward more and more digitization. Demand from faculty and students for online educational resources was outpacing their availability from content creators. Libraries had to balance expectations for instruction and copyright restrictions. The DMCA does not just cover P2P file-sharing; it also has regulations concerning technical DRM tools and anti-circumvention.

Instructional Materials—UCLA Resists External Pressure

In 2005, the Office of Instructional Development and the UCLA Library began converting licensed DVDs into a streaming format for students to use in their courses. The educational media trade group Association for Information Media and Equipment (AIME), which represents 16 educational film producers, objected in the fall of 2009, claiming that streaming distribution was copyright infringement. AIME claimed that UCLA (and other higher education institutions) could purchase only one copy of a DVD and stream it to an unlimited number of students forever, thereby causing a financial hardship for content creators. UCLA argued that the TEACH Act protects its use of streaming media, allowing fair use of copyright material for educational purposes (Technology, Education and Copyright Harmonization Act, 2002).

The way UCLA responded to AIME’s infringement claim and subsequent lawsuits shares several features with other cases in this study. The AIME case was somewhat simpler; UCLA was not negotiating on behalf of itself and students’ allegedly illegal actions, but did require balancing the interests of internal and external stakeholders. There was also a negative response
to the demands of external stakeholders in the face of legal threats. As with the RIAA and MPAA, UCLA was once again in a position to establish a relationship with a content-producing industry that would demonstrate the university’s efforts to remain in compliance with copyright law, but still exercise the rights granted to them.

In December 2010, UCLA suspended its video-streaming service as a good-faith gesture during negotiations with the trade association. The university’s strategy took some similar approaches to cases in Chapters 2 and 3, drawing on its shared-governance structure. Once again, Executive Vice Chancellor Waugh called for the ITPB and the Academic Senate to form a subcommittee and identify relevant principles for an official position to bolster further arguments. In February, the subcommittee responded with a document outlining 10 educational principles supporting the use of streaming media and other educational content. Vice Provost for Information Technology Davis summarized their position:

University instruction long ago ceased to be bound by the walls of the classroom, and we are obligated to provide students with appropriate instructional content in whatever medium helps to foster an effective learning environment. (Hampton, 2010, para. 2)

In March 2010, UCLA restarted its streaming services, with the caveat that faculty needed to submit in writing the pedagogical reasons for requiring students to use copyrighted works. AIME responded with a lawsuit, lost the first suit, and refilled, but the second suit was eventually dismissed with prejudice. This outcome was noted in several higher education and technology publications, marking a significant legal precedent (Cheverie, n.d.; Parry, 2011; Smith, 2012). UCLA anticipated the wide-ranging effects of this outcome, as it was part of the strategy. From the start, administrators knew the case could mark a turning point for other institutions, demonstrate UCLA’s leadership on the issue, points they made publicly and in their internal discussions about the issue.
Course Websites—UCLA Teaches Copyright

UCLA’s online LMS, CCLE, plays an important role in copyright management for instructional materials. One interesting part of the AIME case is that the major factor allowing UCLA to claim a virtual classroom—that only students enrolled in a course can access the materials by authenticating through CCLE—is the same protection that restricts copyright holders from searching for their own content on CCLE. Although it would be difficult for a publisher to access the LMS to see how their materials are used, the university does make a good-faith effort to identify the copyright status of each file hosted on its course websites. UCLA makes considerable effort to provide outreach, consultation, and licensing help to instructors and support staff. Because copyright exceptions for education and fair use are complicated, misinformation among instructors is common. The university was concerned about instructors assuming that a password-protected course site was an adequate shield against infringement claims, and uploading digital copies of instructional materials without permission was outside the scope of fair use. As one administrative interviewee remarked, “We’re good Samaritans; we’re good citizens and we’re trying to do everything the right way.” In that vein, the university has taken on the difficult task of ensuring instructors know their materials are in the public domain or licensed, or can name the relevant exception. To steer this effort, in 2009 the Library and CCLE funded a full-time copyright and licensing librarian to provide expertise across campus. Campus counsel also partnered with the Library to create educational materials and training. They took a similar approach in faculty education to that taken with students by focusing on ways to protect their own work as well as respect the work of others.

A rather permissive approach to fair-use decisions complicates outreach efforts because fair-use exceptions for education have a few main tenets but are typically decided case by case. Despite the complexity of fair-use decisions, the UCLA Library works to instruct and consult on
issues as they arise, rather than making a sweeping statement that would err on the side of always requiring permission from copyright holders. Although this process is inefficient in staff time, it is a point of pride that the university invests time to encourage instructors to know and exercise their rights. An interviewee mentioned that the investment can pay off in licensing costs by making the greatest use of as many legal materials as possible.

**Conclusion**

The case of the DMCA at UCLA is a particularly good example of the ways stakeholder relationships fit into the policy context and their role in mission fulfillment. As I assembled the narrative, a few additional themes surfaced continually. Foremost, a sense of pride in the university’s approach was palpable, even more than in the other two cases. With the ECP and privacy issues, interviewees clearly identified personally with the principles and some were quite satisfied with the results of policymaking. However, this case carried an added element of victory. Participants acknowledge that UCLA’s approach was not perfect, but asserted that it is consistent with ideas and responsibilities they hold dear. They were proud that the university stood up to corporate interests and refused to be a wealthy easy target. They considered their strategy to be successful (rightfully so, as no evidence contradicts that success) and were pleased they had crafted a policy befitting their unique university.

I believe policy context directly enables this sense of pride. Within the policy environment, the university has been able to make policy consistent with its values, rather than simply bowing to the demands of outside stakeholders. UCLA took its core educational mission quite seriously in this case, finding teachable moments for its own members and going so far as to reflect those lessons back to the stakeholders exerting the most pressure. This was the university at its most evangelical and most defiant, rallying its considerable influence and pushing back against commercial interests in the name of academic freedom (Hampton, 2010).
The policy context has enabled UCLA to present and fully contextualize its role and position, allowing the university to project itself as both a creator and consumer of intellectual property and yet maintain its intellectual and pedagogical priorities.

One of the most important reasons UCLA has had success with a strong principled position was because of a decision-making tendency toward cultivating buy-in among the broadest possible range of stakeholders. The university leveraged its IT governance structures to express values. It also invested time in widespread consultation across the community, rallied supporters, and considered feedback from both campus and external stakeholders.
CHAPTER 5

AN ANALYTICAL FRAMEWORK FOR POLICY CONTEXTUALIZATION

Historical Narrative as Policy Context

I had two options to contextualize IT policy at UCLA—I could look to the past or investigate the current environment. I knew that relying on participants’ memories and patchwork documents could result in a shallower, less comprehensive analysis than using present-day sources. However, the benefit of historical data in this study is that it reveals the importance of time in higher education IT policy, which is nearly always struggling to meet challenges presented by technological progress. The BruinCard example from Chapter 3 demonstrated that the passage of time can cool protest, benefitting administrators who “wait out” faculty objections, rather than addressing their concerns. The Data Governance Task Force example from the same chapter showed that the time it takes to progress from committee charge to final report is often underestimated, unduly delaying necessary action. When the committee was formed, UCLA was showing proactivity by bringing to light student data issues, but in the intervening year and a half, the problem has become more pervasive and the university is reacting. Time has also been an important element in the study as a whole; the historical data contributed to policy context analysis by signifying the environment’s dynamic nature. This chapter discusses the crucial patterns that emerged from the narrative, including dominant themes and repeated tactics. The last section focuses on those patterns over time, by applying the framework in more recent events.
Framing IT Policy Context

As discussed in Chapter 1, institutional culture and IT infrastructure are a foundation of the institutional IT policy environment. But further contextualization is necessary to fully understand the elements that shape that environment and foster IT decision-making. In the preceding chapters, three key themes—values, governance, and stakeholder relationships—have emerged as essential elements of UCLA’s historical IT context over the last two decades. Although a different element has weighed heavily in each case, all three have been at work in each. In fact, the cases have demonstrated that the elements are inseparable and co-determining. The complex relationships among the three suggest that institutional values, governance, and stakeholder relationships can be represented as a holistic framework with three connected dimensions, as depicted in Figure 3.

![Policy Context Framework](image)

Figure 4: Policy context framework

This study’s policy context framework binds the three elements into a set of phenomena, with one dimension of the shape representing each contextual element. Because they are linked, any element that experiences significant change will cause the other two elements to shift as well. Figure 4 depicts the policy context with each component equally represented, but, as shown in this study’s cases, the shape shifts as the relative importance of each changes over time.
Regardless of the dimensions, all three are held in tension to create the space inside-the policy context.

It is often said that policy is not (or should not be) created in a vacuum. Because IT policy-making at the institutional level is a complex process, the framework attempts to capture conceptual interrelationships in a meaningful way. The constant tension among the three elements must sustain the space created by the dimensions. In the following sections, I discuss how the case studies in this project, each of which illustrates one dimension of the framework, join and work together in a holistic approach.

The Importance of UCLA’s Mission and Values

When contextualizing IT policy at UCLA, it is important to consider the extent to which the institution’s mission has shaped and given purpose to IT policymaking. The mission statement is not merely a set of platitudes; the values and commitments it espouses have been integral to UCLA’s institutional culture and work. The mission identifies education, research, and service as the institution’s core responsibilities. Education entails teaching and learning in a “community of scholars” that is “engaged together in discovering and advancing knowledge and practice.” Research includes elements of discovery, creativity, and innovation in a place that “advances knowledge [and] addresses pressing societal needs.” Service promotes civic engagement by educating future leaders and instilling skills and social responsibility in all of its members. Each component exists simultaneously and enhances the others. “UCLA endeavors to integrate education, research and service so that each enriches and extends the others” (UCLA, n.d.).

The responsibilities in the mission statement clearly reflect UCLA’s strongly held values. Academic freedom was frequently mentioned by interviewees, including “open access to information, free and lively debate conducted with mutual respect for individuals, and freedom
from intolerance.” But many other values were also expressed in documents and interviews, sometimes linked specifically to IT and policy. Interviewees frequently cited privacy, transparency, stewardship, cooperation, and collaboration, among other values. But these more specific values can also be seen as variations on, or manifestations of, the main values that comprise academic freedom.

All three case studies illustrate the influence of the mission and UCLA’s institutional values. In the DMCA case, for instance, while other universities were locking down or monitoring their networks and punishing infringers, UCLA invoked its social responsibility and rejected a policing approach in favor of offering students lasting guidance. The UCLA Privacy Statement invokes mission and values explicitly:

> Academic and intellectual freedom 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 these values possible and is strongly supported by UCLA. (UCLA Advisory Board on Privacy and Data Protection, 2011, p. 2).

The ECP and the DMCA policies, as well as other supporting documents, use similar language (though few so eloquently).

**UCLA’s Scale and Scope**

UCLA’s size and organizational complexity have also shaped its policy context. As noted in Chapter 1, UCLA is unique on several counts in the UC system, and even among higher education institutions in the United States. For example, UCLA has the highest enrollment. The medical school is the second largest of five in the UC system and partners with UCLA Heath’s extensive network of clinical healthcare providers in the Southern California region. This scale provides UCLA with some advantages, such as a broad base of technological innovation, but its
size has imposed requirements and restrictions that might not constrain smaller and more flexible higher education institutions. Additionally, UCLA plays a distinctive role in the UC system as a provider of technological support to the Office of the President as well as UC Merced (the newest campus). Thus, UCLA’s policies and approaches have a direct influence on other parts of the system. An interviewee opined,

I think the rest of higher ed. can afford to take a stronger single-vision stance. They don’t have to be concerned with this sort of 360-degree view of all the things that concern them. UCLA is such a big place. How many institutions can say that they’re involved in all of these things?

Several interviewees stated that scale and complex responsibilities exert a practical influence on UCLA’s unique ideology, so that institutional values shape the approaches to technology policy and also reaffirm them.

These factors have worked together to create a decentralized organizational structure and operational environment, and a correspondingly distributed decision-making and shared-governance environment. For the most part, this is intentional; UC’s Office of the President recognizes that policies can apply to the whole system, but that they need to be flexible enough for local interpretation and implementation. UCLA administers the campus the same way, with room for various schools, departments, and units to apply campus policy. Stakeholders strongly sense that a single solution cannot address the needs of every component of the organization, and that local autonomy is required.

The case studies demonstrate that although UCLA is in some respects a unique institution, a few key factors have emerged as essential aspects of its institutional IT policy context. These factors implicate one another and are co-determining in the framework. These factors are perhaps not unique to UCLA, and the three-factor framework might apply in other institutional settings, particularly if UCs decentralized structure is considered beneficial.
As you know, UC is a remarkable, remarkable creature, unlike anything anywhere else on the planet and part of the strength of that, and I truly believe, is that the ten campuses and the five academic medical centers and the labs and all the other parts of this are so very different and we have so many strengths we bring to bear and sometimes it can seem like we’re this random collection and have a common label on top of it, but that’s the worst part of it; the best part is when we actually do come together.

While UCLA is certainly unique, the campus has the most diverse range of organizational components among the system campuses, and thus has confronted a wider range of policy challenges. Interviewees confirmed this when discussing their leadership roles in and outside the UC system.

It’s kind of true, and often fair to say, that if you can solve a problem here, you can probably solve it anywhere else because we have a pretty extreme decentralization and distributed environment. And it is challenging, and when I go to national meetings and things, and I talk to colleagues, sometimes their problems just seem trivial. And it’s not that I think their problems are trivial, and I don’t mean to demean what they’re facing, but they just don’t have this overlay of having to deal with this kind of environment; it’s just much more straightforward.

Other campuses would likely not benefit from a wholesale adoption, but UCLA can serve as a valuable source for many particular situations.

**A Holistic Approach to IT Policy and Issues**

**Addressing Multiple Interests**

Often, UCLA’s fusion of values and responsibilities mingle with the pressures from a variety of stakeholders’ interests. When IT policy issues arise, simple solutions are often not an option. The university needs approaches that incorporate its bevy of responsibilities, values, governance approach and varying stakeholder interests. Basically, this study has shown that UCLA uses what I am calling a holistic approach to policymaking. Recalling the university mission, a comprehensive approach makes sense. To engage education, research, and service in the whole community, policies must be diverse and flexible, framed by a diverse set of values.
When policy conflicts arise, the university’s worldview directs decision makers toward an approach that takes multiple competing forces into consideration, with the aim of benefitting the institution, its members, and its partners. Returning to the three-dimensional diagram, the holistic approach shapes the imagined space created by the three-dimensional structure, which to different degrees in different cases, balances values, governance structures and practices, and stakeholder relationships, as depicted in Figure 5. In the diagram, the holistic approach is represented by the lines connecting each element; the holistic approach is an attempt to address all three at once. The holistic approach encourages decisions that are consistent with institutional values, fit within the governance structures and processes, and satisfy multiple stakeholders’ interests.

![Diagram showing the holistic approach in policy context framework]

Figure 5: The holistic approach in the policy context framework

An investment in process is another hallmark of the holistic approach, as a point of pride and part of the university’s identity. Several interviewees acknowledged that UCLA’s process is slow and often inefficient, but they see a greater value in inclusive strategies and measured processes that are sustainable over time. Interviewees lamented the time and effort required to gather input, foster discussion, weigh possibilities, and make decisions for the good of the community, but they also rejected the alternative—the prospect of quick tactics and hasty
decisions made by administrators were distasteful in comparison. Whether or not IT policymakers personally agree, they know the holistic approach is the best route to success in the community.

You’ve got everyone in the room and they can’t make a decision, and there are just so many people in the room! But it’s a better way. And it’s the university’s way to approach a problem, that in the end, and yeah, it might take you a long time to get there, and people won’t be fully happy with the outcome, but it will have everybody’s input and it will be reflective of all the varying things that we need to reflect.

Whereas, as much as people complain about the process of working things up the way we work, people don’t complain when you get to the end point because I’ve had my say and if I didn’t participate, shame on me because I had my option to participate. And if I choose not to then I’d better keep my mouth shut.

Although not all interviewees used the term “holistic,” the pervasiveness of values and mission were clear in their accounts. Participants repeatedly used values-based language and articulated an acceptance of responsibilities that sometimes extended beyond their job titles, in service of the mission. Not every participant was enamored with every policy or process; however, no interviewee indicated that their everyday experience did not match the university’s focus, or that anyone was actively undermining values or mission. Internalization may be a factor that helps explain why stakeholders value participation and why the IT processes explored in this project tended to follow similar patterns.

**Bottom-Up Policymaking**

Another characteristic of the holistic approach is a tendency toward bottom-up policymaking. Multiple interviewees confirmed that often, policy handed down from the Regents was not a good fit locally, and created resistance. The inclusive nature of the holistic approach means that the resulting policies tend to be more comprehensive and representative of the intuition’s culture. The participatory nature of this method allows for many voices, and members who do not contribute have a more difficult time protesting the results. This process does not
usurp all dissent or make a perfect policy for everyone, but it gives decision-makers a consistent justification.

Right, [the campus] is so big that it makes it hard, but in the end, people feel good about having participated. I think that’s a really big part of who UCLA is. You can’t issue from above. It just doesn’t work. You need to have people building it from the bottom and moving it up.

It is here where the university’s investment in process is clear; bottom-up policymaking is slow because it requires discussion and cooperation among community members before making decisions. Of the three cases, the Privacy Board illustrated this best. Interviewees recalled complaints about the effort needed to gather all relevant parties, communicate goals, decide on a course of action, foster effective discussion, and synthesize that discussion into useful policy. However, if all of those steps were not adequately followed, participants suggested that it was more likely that the effort would be waylaid by discussion outside the necessary scope, or fail to meet policy goals. Although a bottom-up decision-making process may be arduous, participation is a key element of the stakeholder buy-in necessary to make shared governance work, and to create lasting and effective policy.

However, it would be a mistake to overstate administrative-faculty harmony. The cases presented here also revealed situations in which faculty strongly advocate their values and interests within the process and governance structure, but ultimately were forced to capitulate. The BruinCard was one example; faculty resistance eventually gave way to the new system that was implemented as a fait accompli. In turn, the issue motivated the Privacy Board’s founders, who chose not to further challenge the BruinCard, but to create a space where similar issues would be subject to faculty review prior to implementation. In a more recent example, the administration took a different approach with Opus by including faculty in the planning processes, but despite faculty reservations and objections, the project has also continued with
very little modification. Email outsourcing to Google was another example; in that case, the university delayed implementation for a few years in attempt to allay faculty concerns, but ultimately adopted the outsourcing plan. pursued the plan. In these cases, technology adoption persisted despite faculty criticism and dissent.

**Holistic Approaches in the Policy Context Framework**

To coexist, the three elements of the IT policy context are in a constantly dynamic relationship. Negotiating those interrelationships is key to the holistic approach, and participants and stakeholders must meet a few conditions. In the interest of inclusiveness, the approach must engage the whole UCLA “community of scholars.” It must encourage a free exchange of information and dialogue. In light of education, research, and service responsibilities, the approach should allow for discovery, foster innovation, and contribute to society. These are lofty goals for any given policy process, and none of the cases examined in this study perfectly fulfill them all. But in each case, efforts to address multiple goals were relevant.

When approaching IT issues holistically, UCLA considered the three elements together. The university considered how a particular policy decision reflects the institution’s values. It determined which existing or proposed governance structures and processes might put those values into practice. It reflected upon the nature of stakeholder relationships, whether they were internal or external, their short- or long-term association, and potential leadership roles. In some cases, relationships lasted only as long as stakeholders dealt directly with the university, such as contracts with hardware or software vendors. But it exerted long-term influence when it encouraged other institutions to adopt similar values or approaches.

In these cases, the university did not always consider the three policy elements in the same order, nor assign them the same weight, something that is clearer when viewing the milestones through the contextual framework. In the ECP case, the relative weight of privacy and
security values have fluctuated over time, with privacy taking precedence in outsourcing issues, but challenged during breach incidents. As mentioned in earlier chapters, privacy and security were not originally set up as opposing forces in the ECP, though in reality the elements have tended to swing like a pendulum, typically in conjunction with shifting governance processes and stakeholder influences. Here, the framework is a reminder that the holistic approach requires constant tension among the three elements; maintaining the shape is easiest when at least one element is stable. For UCLA to successfully venture into an era of data governance, it will need to rely on an already-existing balance of privacy and security values, so that it can focus on new governance processes and increasingly complex stakeholder interests.

The Privacy Board case is an example of how the elements operated in cycles with broad, long-term issues. First, the ITPB, the existing governance structure, identified the need for a new committee to address issues not addressed elsewhere. Members of the resulting body wrote the value-based UCLA Privacy Statement, which will continue to influence policy into the future. Eventually, the Privacy Board took a leadership role in the UC system, impacting the governance relationships among campuses. Meanwhile, policy revisions and implementation strategies continue as more privacy and data-protection issues capture institutional attention.

In the case of the DMCA, UCLA considered the elements in succession. From the original federal legislation, UCLA campus policymakers drafted policy for the campus. Then, policymakers implemented the policy in a new way through existing governance structures. Finally, they shaped relationships with content creators to accommodate the university’s values and policies. Eventually, those relationships spread as examples to other institutions.

Understanding how the contextual elements operate together over time is helpful, but no matter the order, they are ultimately just variations of the codetermining interrelationships among the three elements. As a set, they constitute the framework for decision makers to meet
their many goals while keeping institutional values in sight. Together, they form the basis of an inclusive strategy that allows creative solutions to emerge from open discussion, all in service of the university’s mission.

**Teachable Moments in the Holistic Approach**

UCLA is an educational institution concerned with more than merely teaching its students, but also itself and society at large. The mission statement clearly defines the university’s role: “UCLA’s primary purpose as a public research university is the creation, dissemination, preservation and application of knowledge for the betterment of our global society.” Sensing and using “teachable moments” in IT-related issues is a touchstone of the holistic approach. In elementary education, the teachable moment is the “unplanned opportunity that arises where a teacher has an ideal chance to offer insight to his or her students” (“Teachable Moment,” n.d.). In UCLA’s holistic approach, the unplanned opportunity happens outside the classroom and the institution is the teacher. This phenomenon of UCLA taking an active teaching role occurs regularly in its IT-governance practices. When the method is working, players see problems as opportunities to gain knowledge and spread it widely.

In the policy context framework, teachable moments are represented as points inside the 3D shape, a specific characteristic of the holistic approach, as seen in Figure 6.
As depicted in the figure, the holistic approach’s teachable moments can occur at any point in the policy context framework, relative to relevant elements. For example, the teachable moment of UCLA’s student life approach to illegal file sharing are located near the juncture of values and stakeholder relationships because those were the two most influential elements on the moment, though governance played a part as well. The teachable moments during the Privacy Board discussions are depicted near the center of governance and values elements.

Stakeholders seized teachable moments at several points in the policy events analyzed in this project. For instance, in the case of the DMCA the teachable moment is most obviously directed toward the students as part of the desired outcome. But the teachable moment also occurred in the relationship with external stakeholders, when UCLA took the opportunity to enlighten content creators about privacy values and informed them that the university would be dictating the terms of its own compliance. Those are also instances of UCLA teaching itself; a phenomenon that shows a degree of self-awareness.

When researching IT policy, the framework may not be initially clear. Because UCLA employs teachable moment tactics again and again, they are a signal of its holistic approach.
Teachable moments offer a way to observe the three elements at work, providing contextual insight before the framework is well-defined.

**UCLA Teaches Student-Life Lessons**

UCLA’s DMCA strategy names the first infringement warning as the teachable moment, the point when a student learns that file-sharing is illegal, that IP addresses can easily be tracked on campus and mapped to individual computers, and that financial and academic repercussions for violating the law may emerge. From their one-time break, they learn that the university has given them a limited protected environment to make and learn from their mistakes. They are also continually and thoroughly educated from several sources about intellectual property law and legal alternatives to piracy. UCLA reserves stronger sanctions for those who have not learned from the process. The university believes that encouraging students in this closed environment instills positive values and influences positive behavior for them to carry into the future.

**UCLA Teaches External Stakeholders**

During the process of deciding how to address student file-sharing in residences, stakeholders identified other teachable moments, even if they did not explicitly label them as such. An example is the series of meetings with record and film studio executives, when faculty members took a principled stand and made a case for their student-conduct approach. By including the voices of faculty who were well-equipped to explain and argue for their institutional values, the university took a time of critical opposition by the industry and worked to turn it into an opportunity to instruct external stakeholders in the ways of academia. One faculty interviewee described how difficult it was to explain why content monitoring and restricting access to data produces a chilling effect on scholarship: that it was like “talking to aliens from another planet.” By calling on the faculty, the administration could provide a united
front, one with some particularly strong faculty voices. When some industry representatives offered to install tracking software on the UCLA network, they assumed the university would jump at the chance to outsource student policing, and were confused to get the opposite response:

And I asked, “Are you serious? Do you really think this is appropriate?” And then they finally said, “Well what do you think?” And nobody wanted to say anything. And after an appropriate amount of dead silence, I finally said, … “Other than over my dead body?” And you know, again, sometimes you just have to say those kinds of things. I’m not sure if I didn’t have tenure if I would have said that. Cause it wasn’t exactly a polite thing to say to the MPAA people and the others who were in the room. But it certainly let them know.

By allowing the faculty to speak directly to external stakeholders, administrators could prove they were not simply stonewalling for the sake of being oppositional, and that their position had merit because it was rooted in a purpose different from other ISPs and corporations.

**UCLA Teaches Other Institutions**

The university took another teaching opportunity in its second DMCA testimony in 2007. After summarizing more details about the UCLA quarantine and outreach measures, Davis shared statistics used to measure its success. UCLA assesses its DMCA strategy partly with recidivism rates. The university acknowledges it has flawed data because the studios do not disclose their methods for tracking copyrighted material nor the percentage of notices they send. For instance, after experimentation, UCLA administrators estimated that the MPAA is only passing through as many as 20% of complaints. With available data, the university calculated that first-time offenses dropped dramatically, and second-time offenders dropped from 20% to 2%. Third-time offenders have been extremely rare as well, with only a few students ever receiving academic sanctions. The university noted that the possibility of not graduating or being rejected by a graduate school was a more effective prevention against piracy than the threat of fines or legal action.
UCLA spread its message further through higher education publications. From 2002 to 2008, then UCLA’s Information Technology Policy Security and Policy Coordinator Wada published articles giving advice to other institutions about how to think through illegal file-sharing issues and devise strategy. Perhaps unsurprisingly, the articles include several components of UCLA’s strategy, such as the student judicial process, teachable moments, and student outreach campaigns (Wada & Simon, 2002; Wada, 2008b, 2008a). By offering its model and the reasoning behind it, UCLA asserts itself as a technological leader in higher education.

**UCLA Teaches Itself**

UCLA not only directs its philosophy outwardly; the university also takes opportunities to teach itself by evaluating its assumptions and the efficacy of its programs. The 2008 partnership between the MPAA and Anderson’s Applied Management Research Program mentioned in Chapter 4 fostered communication between the two sides, but also inspired changes in UCLA’s methods. UCLA’s Anderson School used its Applied Management Research Program to study beliefs and attitudes about digital entertainment and file-sharing. Insights gathered from that research led to increased outreach efforts and mandatory educational workshops during orientation and first-time offenders. From students’ survey responses, the university also realized that the issue was not entirely one of ethics, but that students were not always as technically savvy as administrators assumed, and needed technical support to manage file-sharing software and network connections.

More self-assessment in 2010–2011 yielded data that led to further refinements. The university updated the Get Legal website with additional information including workshop information and links to legal-content providers. A Twitter account disseminated information and offered vendor discounts. The university commissioned an undergraduate student to create two educational videos to be posted online and shared with other institutions (UCLA, 2012).
Teachable Moments in Privacy Discussions

Teachable moments were more overt in privacy-related discussions, particularly as the implications of ECP evolution surfaced and as the university applied privacy principles. Outreach became increasingly important to ensure that policy and principles did not survive only on paper, but became part of practice. In these cases, UCLA taught employees by spreading knowledge about rights and expectations related to privacy and data protection. These efforts borrow a tactic from the DMCA case by stressing the role of academic freedom and intellectual property in faculty and students’ academic careers.

In UCLA’s Privacy Statement, the “Considerations for Individuals” section offered plainly-worded advice to employees about protecting their data, not just on behalf of the university, but for themselves. This section falls outside the purpose and tone of the rest of the document, but establishes a basis for future OIT educational efforts, indicating the desire to craft clear principles for the university at large, but also giving useful advice to community members about how they are impacted and what they can do to protect their privacy interests. The section reminds end users that they may use services for incidental personal purposes, but cautions them against using the same accounts for business and personal purposes. The document briefly explains the risks of using third-party e-mail or cloud services without university contracts. Without explicitly prohibiting their use, the policy maintains that “each individual must take responsibility when making decisions about when it is and is not acceptable to use these free/low cost services.” It also reminds end users of an important and very frequently misunderstood point—that “all legal and university policy requirements apply to all University records, whether on UC or non-UC systems” (UCLA Advisory Board on Privacy and Data Protection, 2011, p. 8). It addresses a common misconception that using Google e-mail, for instance, means that those records are not subject to Public-Records Act requests or other university inquiries.
The OIT worked to more widely disseminate this information, but has been challenged in a decentralized environment, especially when new services become available faster than they can educate end users about how they work and the implications of using them. OIT led workshops and events to provide user-friendly information and advice about data privacy and protection. However, attendance is voluntary and tends to draw those who are already interested in the topics. Reaching faculty and staff who are less attuned continues to be challenging for central offices like OIT as well as local technical-support units.

The Privacy diagram included in Chapter 3 was primarily the work of UCLA’s CPO. Initially, it was an attempt to clarify and organize the ideas and definitions in the privacy principles. UCLA’s leadership role in crafting those principles for the UC system eventually led to it being included in the Security and Privacy Initiative’s final report. Even during its development, the diagram was a teaching tool for the institution, guiding and then reflecting the framework discussions in Privacy Board and then UC Steering Committee meetings. A few versions of it circulated during drafting stages of the UCLA Privacy Statement, because it was refined as the university’s conceptualization of privacy matured. At various times, the diagram was repurposed, often for employee training or privacy-related presentations.

**Applying the Policy Context Framework to Emerging IT Policy Issues**

More recent IT policy events suggest how pervasive the holistic approach may be in ongoing IT policy cases. Themes and language from all three cases analyzed in this study have emerged as regular and even expected components of the decision-making process. For example, in 2012, the joint Senate-Administration Task Force on Academic Freedom wrote the “Statement on the Principles of Scholarly Research and Public Records Requests,” a document that neatly ties together the mission and the university’s wider role:
Faculty at UCLA carry out a triple mission of teaching, service, and research. The three parts of this mission are not identical: our service to the institution is by definition something that concerns the shared governance, operation, and decision-making here at UCLA and UC wide. By contrast, our research and teaching are often conducted in collaboration with others in our discipline at institutions around the world, and serve the general advancement of knowledge. UCLA Senate-Administration Task Force on Academic Freedom. (2012, sec. The principles of scholarly research)

This document depicts faculty as stakeholders with internal and external interests, and describes how academic freedom values are essential to both—shared governance for service and global collaboration for knowledge advancement. As the university continues to recognize the three IT elements, the framework provides analytical guidance for understanding their organization and connections. Two recent IT issues provide an opportunity for framework application.

**UCLA’s Online Education Initiative**

Since the early 2000s, IT policymaking at UCLA has steadily attempted to balance values, governance process, bottom-up distributed decision making, and diverse stakeholder interests. These elements were in play when UCLA responded to the UC Regents’ advocacy for online education to be adopted by all campuses in 2013.\(^\text{12}\) The Regents’ plan was met with considerable opposition from the UCLA community. As demonstrated in Chapters 3 and 4, UCLA’s holistic approaches tend to include institutional research and consultation with various on-campus experts before implementing new programs. Even when policymakers cannot achieve full consensus, they look for a significant degree of buy-in from multiple stakeholders. When the UC Regents implemented an initiative for campuses to include online education in their undergraduate programs, it seemed to lack the considerations most important to UCLA, and decision makers bristled.

I contrast [a holistic approach policy] with what just happened during the most recent Regents meeting where they said, “Oh yeah, we need to do online education.” Like,

\(^{12}\) [http://www.ucop.edu/innovative-learning-technology-initiative/]
really? Did someone actually do the research to figure out how students learn and what do we need to put into online education to make sure they’re still getting the same educational experience? I mean, to me, this is like, how can higher ed. do that? That’s not how we develop policy, that’s now how we make decisions, we actually research it first!

In response, UCLA conducted its own institutional research and began a lengthy evaluation of implementation. The Executive Vice Chancellor convened the Online Education Steering Committee comprised of Deans, technology support, administrative staff, and faculty to address the issue. In 2014, the Academic Senate’s Committee on Instruction and Technology drafted its “Faculty Guidance for Online/Mediated Instruction at UCLA.” This memorandum clearly grew from the policy context explored in this project. The document is explicit about values, principles, and the mission. It recognizes that collaboration and shared governance are key for a comprehensive strategy that can “move beyond the provision of infrastructure and services, to emphasize the best practices for using those resources” (Committee on Instruction and Technology, 2014, p. 1). As with the DMCA, the university looked within to craft a principled response to pressures from external stakeholders, though this time UC was considered external.

IT policy and strategy regarding online education is complex, much more than it seems at first blush. UCLA was pressured to include online learning in its academic programs for many reasons. Facing state budget cuts, the campus sought to increase enrollment, particularly from out-of-state students who pay higher tuition. But increased enrollment means increased course offerings and a greater demand on limited physical space and infrastructure. The university was also paying attention to pedagogical trends: some instructors and students advocated adopting new technologies to enhance instruction. The visibility of online instruction was also attractive, particularly as a way to shore up UCLA’s reputation as a technological leader:

As a 21st-century public university, the academic “birthplace” of networked computing and telecommunications—today’s Internet—and an early adopter of all types of
instructional technologies, UCLA is keenly aware that these technologies of communication, immersion, search and retrieval, and knowledge creation have helped to transform the very notion of “the public,” the public interest, public institutions, and public engagement. (Committee on Instruction and Technology, 2014, p. 8)

IT units on campus fielded questions and requests from all sides, from administrators focused on efficiency to faculty and students seeking to improve teaching, learning, and research. In my experience, technology support offices have been fielding these questions from many sources, usually in an ad hoc manner. Although UCLA certainly can build or implement the infrastructure and tools required to support online courses, most realize they cannot or should not do so without a cohesive strategy and standards. Effective instruction does not often translate directly to the online environment, even with sophisticated technology. Many aspects of teaching and learning must be redesigned for teachers and students. The Committee on Instruction and Technology’s memorandum summarizes a few of these aspects: (a) Workload and reward structures; (b) creativity, discovery, authorship, and credit; (c) collaboration, collegial relations, and mentorship; (d) instructional evaluation, (e) economics; (f) public engagement, outreach, visibility and reputation; (g) Data protection and stewardship; and (h) academic integrity.

Faculty, in particular, insist that these points should be sufficiently addressed and designed into the development, adoption, and integration of online programs into existing programs.

The Committee on Instruction and Technology’s document evokes academic freedom values when expressing faculty concerns about implications of digital coursework:

Academic and intellectual freedom depend on the ability of any member of the university community to conduct research, inquire, teach and learn without undue or inappropriate constraints on thought and expression—including concerns that those expressions will “live on” in a publicly-accessible data repository long after the program, course, or advising relationship is over. (Committee on Instruction and Technology, 2014, p. 10)

Although the committee understands the pressure to integrate more technological resources, the memorandum stresses that technological mitigation cannot and should not stand
alone; it should be part of a broader effort. For instance, online courses pose an increased risk for academic dishonesty because it may be easier to cheat outside of the classroom than in it. Many technological safeguards are available to mitigate this risk, such as webcams during testing and plagiarism-detecting software, but they should not stand alone.

Although new technical tools such as plagiarism-detection software, identity and document authentication, and webcams may help mitigate dishonesty, they cannot replace strong, consistent, and clearly-articulated expectations of honest and ethical scholarship, cultivating a shared sense of community and responsibility within a class, and instructors focusing on individual students’ performance and learning. (Committee on Instruction and Technology, 2014, p. 10)

Although the word “holistic” does not appear in the document, it is clear that faculty advocate a carefully considered approach that addresses the issue from all sides and fits into UCLA’s institutional culture. The authors also devoted a section to data protection and stewardship that contains much of the same language as the Data Governance Task Force’s charter, referring to “unprecedented amounts of data on student and faculty activities which may be used in unanticipated ways.” They stressed the importance of good data stewardship that “balances interests ranging from the public good, to facilitating scholarly collaboration, to transparency and accountability, to the legalities of intellectual property and contracts.” Data stewardship ties to the entire mission of the university:

Online/mediated instruction thus requires that instructors, administrators, and staff maintain the highest standards of data stewardship, which balance the privacy rights and intellectual freedom of individuals, academic freedom as an integral part of the University’s mission, the security of technical systems and the information they contain, and the legal, policy and administrative obligations of the UC as a public institution. (Committee on Instruction and Technology, 2014, p. 3)

An administrative interviewee supported the collaboration of administrators and faculty in an online-learning endeavor, pointing out that administrators are not likely to be in touch with the details of teaching and learning: how students, instructors, and teaching assistants
communicate. Student voices have also been extremely valuable because their responses were unexpected. When polled, a majority of students initially opposed the idea of online instruction, despite comprehensive adoption of technology in other areas of their lives. A faculty interviewee explained their fear of online education distancing them from their professors: “They busted their butts to get here. They don’t want to see us on TV. Remember, those are … the 10% who actually got in.” To students, going to class on campus is a vital part of their college experience. It was not until they were asked more nuanced questions about how their education could be more effective with technological enhancement rather than replacement that students felt more comfortable with the idea.

In 2014, UCLA’s Undergraduate Students Association Council polled students about online education. The council concluded that the university needs to improve communication about online initiatives, particularly about different ways to integrate online instruction, such as hybrid courses. They recommended the university view online education “as an enhancement; it’s not a way for the institution to disengage” (UCLA Faculty Committee on Educational Technology, 2014, p. 1).

Anecdotes like this demonstrate the importance of having “all the right people in the room.” An administrator participant believed the original UC committee did not have all the right people before they handed down the mandate to offer online courses. Even in the institution, “all the right people in the room” refers to several different rooms of several committees, some of which have overlapping membership. Again, the investment in process has slowed widespread adoption of online instruction. In my experience, many instructors, department heads, and deans have expressed interest for their own programs and clearly would like to explore the option more, but are wary of the implications as campus committees have clarified the concept.
UCLA Heath System’s Cyber Attack

The historical policy context, particularly from these three cases, brings patterns to light in the university’s reaction to a recent cyber attack. In July 2015, UCLA Chancellor Block announced that hackers had accessed a UCLA Health system network that hosted sensitive information on approximately 4.5 million patients (Block, n.d., para. 1–2). Though there was no evidence that attackers had accessed or acquired personal information, the potential implications were disastrous.

This study’s analytic framework is a helpful guide to understand the impact of the attack on campus, by highlighting the contextual elements and the university’s strategy. In the months that followed the attack, UC clearly took a holistic approach. First, UC hired an outside cybersecurity firm to assist with a response, an external stakeholder which, to some degree, assumed the role of an internal stakeholder. UC’s Office of the President also established a new shared governance structure; the Cyber-Risk Governance Committee, which consists of representatives from across the system and the Academic Senate to oversee and guide strategy. Additionally, in the obvious recognition of a teachable moment, UC implemented mandatory cyber security training for every employee.

The issue has other traits in common with this study’s cases, such as faculty concern over the state of their valued privacy protections. During the fall after the attack, UC and UCLA administrators assured campuses that they would be implementing increased security measures. However, faculty alleged that they had done so without appropriate consultation, in violation of shared governance practices. In January 2016, UC Berkeley professor and Academic Senate-Administration Joint Committee on Campus Information Technology member Ethan Ligon emailed his colleagues, warning them that new monitoring systems had been installed on all UC
Ligon claimed that UC administrators had asked for committee members to not share the information widely, but that a group of faculty felt that, “continued silence on our part would make us complicit in what we view as a serious violation of shared governance and a serious threat to the academic freedoms that the Berkeley campus has long cherished” (Jaschik, 2016, para. 3).

When word spread, faculty leaders were dismayed that the security system had been deployed in a top-down governance action, without consultation from the typical faculty committees. They articulated their concerns to university administration and the press. On February 1, UC President Janet Napolitano responded with a letter assuring that the university did not have a “secret initiative to snoop on faculty activities” (Napolitano, 2016 para. 1). She emphasized the necessity of cyber threat detection, claimed that UC had appropriately disclosed its strategies, and engaged faculty via faculty representation on the Cyber Risk Governance Committee.

In conjunction with the letter, UC released a document highlighting the portions of the ECP specifically pertaining to network security activities, with a few sentences of summary for each (University of California Office of the President, 2016). An additional letter was issued by UC’s Chief Operating Officer Rachael Nava, speaking to concerns about privacy violations. Nava wrote that she did not see a conflict between privacy protections and cyber security measures, arguing that they “reinforce each other in crucial ways.” She stressed: “While the ECP
establishes an expectation of privacy in an individual’s electronic communications transmitted using University systems, it tempers this expectation with the recognition that privacy requires a reasonable level of security to protect sensitive data from unauthorized access” (Nava, n.d., para. 2, 9). The letter relays general information about UC’s strategy methods to avoid violating privacy protections, including restricting the type and amount of data reviewed, prohibiting collected data reuse, and adhering to the least perusal principles in the ECP.

UC administrators refused to disclose comprehensive technical details about the new system, citing ongoing litigation and the danger of sharing protective techniques. The university was and continues to be under immense pressure from external stakeholders in this issue. As of February 2016, seventeen class action lawsuits were filed against UC and UCLA. Additionally, the university was at risk of fines levied by the state of California for failing to adequately protect sensitive data. National press brought attention to the issue beyond the typical stakeholders, damaging the university’s reputation on a wide scale.

Despite reassurances that stronger cyber threat detection systems are not a threat to privacy protection and the balance established by the ECP, the issue represents a shift in attention toward security values, one that privileges operations over vision. An interviewee pointed out that UCLA Health had previously not implemented this new level of traffic and content monitoring, in deference to the ECP. By deploying it later without changing the policy, it there clearly was a change in the policy’s interpretation. UC has not explained that shift, saying only that the new system is “entirely consistent with the letter and the spirit of the ECP” (Napolitano, 2016 para. 5). The document containing the ECP’s security provisions is arguably proof of the ‘letter,’ but is less convincing about the ‘spirit.’ Certainly, there is a valid argument that UCLA’s security protections were inadequate, and change was necessary. In breach situations, there is merit to a swift response. However, this is a case where historical
contextualization is most valuable, because it exposes patterns. As covered in Chapter 2, The ECP has been revised twice to make small but meaningful allowances for security-related monitoring. Earlier in this chapter, I referenced examples of faculty members expressing privacy concerns, but ultimately ceding ground to operational objectives. In this case, the faculty complained not only about the measures themselves, but that the university had eschewed the typical investment in process in favor of responsiveness. I do not argue that it was the wrong decision, but that a more inclusive approach (even after the fact) would have lessened the threat to faculty trust.

While case is not the death knell for privacy at UC or UCLA, a change in policy interpretation signals a contextual shift. From here, it is not difficult to imagine a policy environment in which privacy protections gradually erode and operational considerations take precedence over academic freedom values, with or without new policy. If that result is not in the best interest of the educational mission, the university will need to realign its policy elements.

**Conclusion**

This study of IT policymaking context and approach at UCLA has built upon institution and infrastructure theory and three historical case studies to propose a holistic framework for analyzing technology policy phenomena. I have identified three central components of IT policymaking—values, governance, and stakeholder relationships—that have shaped IT policy at UCLA. The case studies presented here have demonstrated the interdependent relationship of the three elements.

In the ECP case, institutional values came to the forefront in the policy context. I argued that a mission-driven university like UCLA strives to consistently fulfill those values through technology policy and strategy. In the Privacy Board case, governance structures and processes
were the pivotal elements, enabling institutional values to be expressed through practice. Governance principles, particularly UC’s shared governance model, are reflected in the purposes and structures of the governing bodies. In the DMCA case, UCLA’s stakeholder relationships took center stage as the interests of multiple internal and external stakeholders were negotiated in attempts to comply with copyright law and satisfy the entertainment industry without compromising the university’s educational mission or institutional values.

Taken together, the three case studies demonstrate the interdependent relationships among three elements in the institution’s policy context and decision-making. Though I presented the cases separately, their narratives overlap in significant ways. Not only were many of these events and controversies occurring at or around the same time, but the decisions about one affected policy for the others. Values shape governance and stakeholder relationships; governance applies and implements values and communicates the university’s interests with stakeholders; stakeholder relationships temper governance processes and can prompt a re-interpretation of values.

By understanding the associations as a three-dimensional framework, it is possible to see not just the mechanics of institutional policymaking, but the interplay for the forces that operationalize them. In such a framework, any one of the factors can be shaped by interrelationships with the others. The DMCA case clearly demonstrated the close relation between values and various stakeholders. The ECP case showed that stakeholder relationships also came into play within UC as an institution. As bad actors continuously develop methods to breach IT security, privacy values experience a squeeze, and the university must decide to address threats within the current ECP parameters, or reconsider its interpretation of values to meet new challenges. It must decide if academic freedom could be better served by a different balance of values.
Governance and external stakeholders have a close relationship as well. Obviously, university policy must comply with federal and state law. External funding sources often dictate the allocation, allowable use, re-use, and destruction of technology resources and research data, issues the Data Governance Task Force is considering. Third parties offering cloud computing and software as a service challenge current standards and practices; vendor agreements must ensure that external companies manage data to the university’s expectations.

The ongoing relationship between values and governance was pervasive through the three cases. A mission-driven institution needs a governance model that consistently serves its values. The governance structures must be able to constantly balance business and academic needs and fairly adjudicate conflicts. It must be flexible enough to meet new challenges and re-interpret values if current methods and approaches need adjustment. The three-dimensional context framework accounts for all these interactions, and provides a method for evaluating technology policy-related phenomena.

Clearly, UCLA is a unique institution with unique policies. I believe that the framework developed here provides insight into other educational institutions as well. Many universities have authoritarian, centralized, top-down governance models that differ widely from UCLA’s. However, that does not preclude the application of the 3-factor framework; the three elements exist in some form in every institution. A small private teaching university may differ from a large state research institution, but it shares a similar educational mission, has a governance structure, and answers to a board of directors or other external stakeholders. It has faculty, staff, student and parent stakeholders and likely maintains a relationship with its community and/or private industry.

The three-element framework provides a way to analyze technology policy processes by concentrating on interactions, regardless of the makeup of each component. Furthermore, a
holistic approach need not mirror UCLA’s to be effective in similar ways. The holistic approach can apply in a top-down policy-making model as well. Even if an institution does not require widespread stakeholder buy-in to create technology policy, thoughtful consultation can ease implementation, as seen in the DMCA case. Likewise, an investment in student behavior as a whole supports critical thinking and ownership, adding value to instruction and encouraging civic engagement.

However, a structurally dissimilar institution may experience challenges when applying the case studies’ lessons in depth. Interviewees described the holistic approach as the only suitable fit for UCLA due to its size, scope, mission, shared governance, and widely distributed technology management. But a standing advisory structure like the Privacy Board could be onerous in a streamlined governance model that requires quick ad-hoc decision-making. A strongly principled stance like the Privacy Statement or the DMCA strategy is overkill in a university with centralized governance and fewer or less diverse external stakeholders. The holistic approach works best in institutional cultures that value an investment in process; its inherent inefficiency would be a deterrent elsewhere.

When applying the framework to another institution, I would suggest that the researcher work from the general to the specific, looking for broad themes across several events, then piecing together how they operate. While doing so, it is helpful to look for one particular element, analogous to UCLA’s teachable moment at the center of the framework. The element is part of a pattern, a common characteristic of the technology decision-making process such as a repeated goal, method, or practice. Identifying where that repeated element occurs within the framework gives clues to the whole shape. Once the three elements and a common element are determined, the framework can serve as an analytical tool for institutional researchers to understand their own policy history and determine the most effective methods for the future.
APPENDIX A
Electronic Mail Policy

University of California
Office of the President
August 1, 1996

TABLE OF CONTENTS

I. INTRODUCTION
   Cautions
II. PURPOSE
III. DEFINITIONS
IV. SCOPE
V. GENERAL PROVISIONS
   A. Purpose
   B. University Property
   C. Service Restrictions
   D. Consent and Compliance
   E. Restrictions on Access Without Consent
   F. Recourse
   G. Misuse
VI. SPECIFIC PROVISIONS
   A. Allowable Use
      1. Purpose
      2. Users
      3. Non-Competition
      4. Restrictions
      5. Representation
      6. False Identity
      7. Interference
      8. Personal Use
   B. Security and Confidentiality
   C. Archiving and Retention
VII. POLICY VIOLATIONS
VIII. RESPONSIBILITY FOR POLICY
IX. CAMPUS RESPONSIBILITIES & DISCRETION
APPENDIX A, DEFINITIONS
APPENDIX B, REFERENCES

I. INTRODUCTION

This Policy clarifies the applicability of law and of other University policies to electronic mail. It also defines new policy and procedures where existing policies do not specifically address issues particular to the use of electronic mail.

The University recognizes that principles of academic freedom, freedom of speech, and privacy of information hold important implications for electronic mail and electronic mail services. This Policy reflects these firmly-held principles within the context of the University's legal and other obligations.

The University encourages the use of electronic mail and respects the privacy of users. It does not routinely inspect, monitor, or disclose electronic mail without the holder's (as defined in Appendix A,
Definitions) consent. Nonetheless, subject to the requirements for authorization and notification defined in this Policy, the University may deny access to its electronic mail services and may inspect, monitor, or disclose electronic mail when required by and consistent with law, when there is substantiated reason (as defined in Appendix A, Definitions) to believe that violations of policy or law have taken place, or, in exceptional cases, when required to meet time-dependent, critical operational needs. These provisions are comparable to those of policies that apply to other forms of communications, such as conventional mail.

**Cautions:**

Users should be aware of the following:

1. Both the nature of electronic mail and the public character of the University's business (see Caution 2 below) make electronic mail less private than users may anticipate. For example, electronic mail intended for one person sometimes may be widely distributed because of the ease with which recipients can forward it to others. A reply to an electronic mail message posted on an electronic bulletin board or "listserv" intended only for the originator of the message may be distributed to all subscribers to the listserv. Furthermore, even after a user deletes an electronic mail record from a computer or electronic mail account it may persist on backup facilities, and thus be subject to disclosure under the provisions of Section V of this Policy. The University cannot routinely protect users against such eventualities.

2. Electronic mail, whether or not created or stored on University equipment, may constitute a University record (see Appendix A, Definitions) subject to disclosure under the California Public Records Act or other laws, or as a result of litigation. However, the University does not automatically comply with all requests for disclosure, but evaluates all such requests against the precise provisions of the Act, other laws concerning disclosure and privacy, or other applicable law.

Users of University electronic mail services also should be aware that the California Public Records Act and other similar laws jeopardize the ability of the University to guarantee complete protection of personal electronic mail resident (see Section VI. A. 8) on University facilities.

The California Public Records Act does not, in general, apply to students except in their capacity, if any, as employees or agents of the University. This exemption does not, however, exclude student email from other aspects of this Policy.

3. The University, in general, cannot and does not wish to be the arbiter of the contents of electronic mail. Neither can the University, in general, protect users from receiving electronic mail they may find offensive. Members of the University community, however, are strongly encouraged to use the same personal and professional courtesies and considerations in electronic mail as they would in other forms of communication.

4. There is no guarantee, unless "authenticated" mail systems are in use, that electronic mail received was in fact sent by the purported sender, since it is relatively straightforward, although a violation of this Policy, for senders to disguise their identity. Furthermore, electronic mail that is forwarded may also be modified. Authentication technology is not widely and systematically in use at the University as of the date of this Policy. As with print documents, in case of doubt receivers of electronic mail messages should check with the purported sender to validate authorship or authenticity.

5. Encryption of electronic mail is another emerging technology that is not in widespread use as of the date of this Policy. This technology enables the encoding of electronic mail so that for all practical purposes it cannot be read by anyone who does not possess the right key. The answers to questions raised by the growing use of these technologies are not now sufficiently understood to warrant the formulation of University policy at this time. Users and operators of electronic mail facilities should be aware, however, that these technologies will become generally available and probably will be increasingly used by members of the community.
II. PURPOSE

The purpose of this Policy is to assure that:

A. The University community is informed about the applicability of policies and laws to electronic mail;

B. Electronic mail services are used in compliance with those policies and laws;

C. Users of electronic mail services are informed about how concepts of privacy and security apply to electronic mail; and,

D. Disruptions to University electronic mail and other services and activities are minimized.

III. DEFINITIONS

The terms electronic mail and email are used interchangeably throughout this Policy.

The following terms used in this Policy are defined in Appendix A. Knowledge of these definitions is important to an understanding of this Policy.

- Computing Facility(ies)
- Electronic Mail System or Services
- University Email System or Services
- Email Record or Email
- University Record
- University Email Record
- Use of University or other Email Services
- Possession of Email
- Holder of an Email Record or Email Holder
- Substantiated Reason

IV. SCOPE

This Policy applies to:

- All electronic mail systems and services provided or owned by the University and
- All users, holders, and uses of University email services; and
- All University email records in the possession of University employees or other email users of electronic mail services provided by the University.

Excluded from the foregoing are electronic mail services of Department of Energy Laboratories managed by the University, and email users of such electronic mail services who are employees and agents of those Laboratories.

This Policy applies only to electronic mail in its electronic form. The Policy does not apply to printed copies of electronic mail. Other University records management policies (see Appendix B, References), however, do not distinguish among the media in which records are generated or stored. Electronic mail messages, therefore, in either their electronic or printed forms, are subject to those other policies, including provisions of those policies regarding retention and disclosure.

This Policy applies equally to transactional information (such as email headers, summaries, addresses, and addressees) associated with email records as it does to the contents of those records.

This Policy is effective immediately as interim policy, with final Universitywide implementation to be
effective January 1, 1997.

V. GENERAL PROVISIONS

As noted in the Introduction, the University recognizes that principles of academic freedom, freedom of speech, and privacy of information hold important implications for electronic mail and electronic mail services. This Policy reflects these firmly-held principles within the context of the University’s legal and other obligations.

A. **Purpose.** In support of its threefold mission of instruction, research, and public service, the University encourages the use of University electronic mail services to share information, to improve communication, and to exchange ideas.

B. **University Property.** University electronic mail systems and services are University facilities as that term is used in other policies and guidelines. Any electronic mail address or account associated with the University, or any sub-unit of the University, assigned by the University to individuals, sub-units, or functions of the University, is the property of The Regents of the University of California.

C. **Service Restrictions.** Those who use University electronic mail services are expected to do so responsibly, that is, to comply with state and federal laws, with this and other policies and procedures of the University, and with normal standards of professional and personal courtesy and conduct. Access to University electronic mail services, when provided, is a privilege that may be wholly or partially restricted by the University without prior notice and without the consent of the email user when required by and consistent with law, when there is substantiated reason (as defined in Appendix A, Definitions) to believe that violations of policy or law have taken place, or, in exceptional cases, when required to meet time-dependent, critical operational needs. Such restriction is subject to established campuswide procedures or, in the absence of such procedures, to the approval of the appropriate campus Vice Chancellor or University Vice President.

D. **Consent and Compliance.** An email holder's consent shall be sought by the University prior to any inspection, monitoring, or disclosure of University email records in the holder's possession, except as provided for in Section V. E. University employees are, however, expected to comply with University requests for copies of email records in their possession that pertain to the administrative business of the University, or whose disclosure is required to comply with applicable laws, regardless of whether such records reside on a computer housed or owned by the University. Failure to comply with such requests can lead to the conditions of Section V. E.

E. **Restrictions on Access Without Consent.** The University shall only permit the inspection, monitoring, or disclosure of electronic mail without the consent of the holder of such email when: (i) required by and consistent with law, (ii) there is substantiated reason (as defined in Appendix A, Definitions) to believe that violations of law or University policy have taken place, or (iii) in exceptional cases, to meet time-dependent, critical operational needs.

When the contents of email must be inspected, monitored, or disclosed without the holder's consent:

1. **Authorization.** Except in emergency situations, such actions must be authorized in advance and in writing by the authority specified by the law or policy under which the action is taken. If the authority is not specified, authorization must be sought from the responsible (see Section IX, Campus Responsibilities) campus Vice Chancellor or University Vice President. This latter authority may not be further re-delegated. University counsel's advice should normally be sought prior to authorization because of changing interpretations by the courts of laws affecting the privacy of electronic mail, and because of potential conflicts among different applicable laws. Authorization shall be limited to the least perusal of contents and the least action necessary to resolve the situation.
2. **Emergencies.** In emergency situations (for instance, when the community or its members are endangered or when access to electronic mail records must be secured to ensure the preservation of evidence), the least perusal of contents and the least action necessary to resolve the emergency may be taken immediately without authorization, but appropriate authorization must then be sought without delay following the procedures described in Section V. E. 1 above. If the action taken is not subsequently authorized, the responsible authority shall seek to have the situation restored as closely as possible to that which existed before action was taken.

3. **Notification.** In either case, the responsible authority or their designee shall, at the earliest possible opportunity consistent with law and other University policy, notify the affected individual of the action(s) taken and the reasons for the action(s) taken.

4. **Compliance with Law.** Actions taken under Paragraphs 1. and 2. shall be in full compliance with the law and other applicable University policy, including laws and policies listed in Appendix B. This has particular significance for email residing on computers not owned or housed by the University. Advice of counsel always must be sought prior to any action taken under such circumstances. It also has particular significance for email whose content is protected under the Federal Family Educational Rights and Privacy Act of 1974, which applies equally to email as it does to print records.

F. **Recourse.** Procedures for the review and appeal of actions taken under Sections V. C, D, and E and under Section VII shall be implemented (or existing procedures adapted) by each campus to provide a mechanism for recourse to individuals who believe that actions taken by employees or agents of the University were in violation of this Policy.

G. **Misuse.** Both law and University policy prohibit, in general, the theft or other abuse of computing facilities. Such prohibitions apply to electronic mail services, and include (but are not limited to): unauthorized entry, use, transfer, and tampering with the accounts and files of others; interference with the work of others and with other computing facilities. Under certain circumstances, the law contains provisions for felony offenses. Users of electronic mail are encouraged to familiarize themselves with these laws and policies (see Appendix B, References).

**VI. SPECIFIC PROVISIONS**

A. **Allowable Use**

In general, use of University electronic mail services is governed by policies that apply to the use of all University facilities. In particular, use of University electronic mail services is encouraged and is allowable subject to the following conditions:

1. **Purpose.** Electronic mail services are to be provided by University organizational units in support of the teaching, research, and public service mission of the University, and the administrative functions that support this mission.

2. **Users.** Users of University electronic mail services are to be limited primarily to University students, faculty and staff for purposes that conform to the requirements of this Section.

3. **Non-Competition.** University Electronic mail services shall not be provided in competition with commercial services to individuals or organizations outside the University.

4. **Restrictions.** University Electronic mail services may not be used for: unlawful activities; commercial purposes not under the auspices of the University; personal financial gain (except as permitted under applicable academic policies); personal use inconsistent with Section VI. A. 8; or uses that violate other University policies or guidelines. The latter include, but are not limited to, policies and guidelines (see Appendix B, References) regarding intellectual property, or regarding sexual or other forms of harassment.
5. **Representation.** Electronic mail users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the University or any unit of the University unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing the University. {An appropriate disclaimer is: "The opinions or statements expressed herein are my own and should not be taken as a position, opinion, or endorsement of the University of California."}

6. **False Identity.** University email users shall not employ a false identity. Email may, however, be sent anonymously provided this does not violate any law or this or any other University policy, and does not unreasonably interfere with the administrative business of the University.

7. **Interference.** University email services shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities, or unwarranted or unsolicited interference with others' use of email or email systems. {Such uses include, but are not limited to, the use of email services to: (i) send or forward email chain letters; (ii) "spam", that is, to exploit listservs or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited email; and (iii) "letter-bomb", that is, to resend the same email repeatedly to one or more recipients to interfere with the recipient's use of email.}

8. **Personal Use.** University electronic mail services may be used for incidental personal purposes provided that, in addition to the foregoing constraints and conditions, such use does not (i) directly or indirectly interfere with the University operation of computing facilities or electronic mail services; (ii) burden the University with noticeable incremental cost; or (iii) interfere with the email user's employment or other obligations to the University. Email records arising from such personal use may, however, be subject to the presumption in Appendix A, definition of a University Email Record, regarding personal and other email records. Email users should assess the implications of this presumption in their decision to use University electronic mail services for personal purposes.

**B. Security and Confidentiality**

1. The confidentiality of electronic mail cannot be assured. Such confidentiality may be compromised by applicability of law or policy, including this Policy, by unintended redistribution, or because of inadequacy of current technologies to protect against unauthorized access. Users, therefore, should exercise extreme caution in using email to communicate confidential or sensitive matters.

2. Business and Finance Bulletin RMP-8, *Legal Requirements on Privacy of and Access to Information*, prohibits University employees and others from "seeking out, using, or disclosing" without authorization "personal or confidential" information, and requires employees to take necessary precautions to protect the confidentiality of personal or confidential information encountered in the performance of their duties or otherwise. This prohibition applies to email records. In this Policy the terms "inspect, monitor, or disclose" are used within the meaning of "seek, use, or disclose" as defined in RMP-8.

3. Notwithstanding the previous paragraph, users should be aware that on occasion network and computer operations personnel and system administrators may, during the performance of their duties, inadvertently see the contents of email messages. Except as provided elsewhere in this Policy, they are not permitted to do so intentionally or disclose or otherwise use what they have seen. One exception, however, is that of systems personnel (such as "postmasters") who may need to inspect email when re-routing or disposing of otherwise undeliverable email. This exception is limited to the least invasive level of inspection required to perform such duties. Furthermore, this exception does not exempt postmasters from the prohibition against disclosure of personal and confidential information of the previous paragraph, except insofar as such disclosure equates with good faith
attempts to route the otherwise undeliverable email to the intended recipient. Re-routed mail normally should be accompanied by notification to the recipient that the email has been inspected for such purposes.

4. The University attempts to provide secure and reliable email services. Operators of University electronic mail services are expected to follow sound professional practices in providing for the security of electronic mail records, data, application programs, and system programs under their jurisdiction. Since such professional practices and protections are not foolproof, however, the security and confidentiality of electronic mail cannot be guaranteed. Furthermore, operators of email services have no control over the security of email that has been downloaded to a user's computer.

As a deterrent to potential intruders and to misuse of email, email users should employ whatever protections (such as passwords) are available to them.

5. Users of electronic mail services should be aware that even though the sender and recipient have discarded their copies of an electronic mail record, there may be back-up copies that can be retrieved. Systems may be "backed-up" on a routine or occasional basis to protect system reliability and integrity, and to prevent potential loss of data. The back-up process results in the copying of data onto storage media that may be retained for periods of time and in locations unknown to the originator or recipient of electronic mail. The practice and frequency of back-ups and the retention of back-up copies of email vary from system to system. Electronic mail users are encouraged to request information on the back-up practices followed by the operators of University electronic mail services, and such operators are required to provide such information upon request.

C. Archiving and Retention

University records management policies do not distinguish among media with regard to the definition of University records. As such, electronic mail records are subject to these policies. In particular, such records are subject to disposition schedules in the University of California Records Disposition Schedules Manual, which distinguishes among different categories of records, from the ephemeral to the archival.

The University does not maintain central or distributed electronic mail archives of all electronic mail sent or received. Electronic mail is normally backed up (see Section VI. B. 5), if at all, only to assure system integrity and reliability, not to provide for future retrieval, although back-ups may at times serve the latter purpose incidentally. Operators of University electronic mail services are not required by this Policy to retrieve email from such back-up facilities upon the holder’s request, although on occasion they may do so as a courtesy.

Email users should be aware that generally it is not possible to assure the longevity of electronic mail records for record-keeping purposes, in part because of the difficulty of guaranteeing that electronic mail can continue to be read in the face of changing formats and technologies and in part because of the changing nature of electronic mail systems. This becomes increasingly difficult as electronic mail encompasses more digital forms, such as embracing compound documents composed of digital voice, music, image, and video in addition to text. Furthermore, in the absence of the use of authentication systems (see Section I, Caution 4), it is difficult to guarantee that email documents have not been altered, intentionally or inadvertently.

Email users and those in possession of University records in the form of electronic mail are cautioned, therefore, to be prudent in their reliance on electronic mail for purposes of maintaining a lasting record. Sound business practice suggests that consideration be given to transferring (if possible) electronic mail to a more lasting medium/format, such as acid-free paper or microfilm, where long-term accessibility is an issue.

VII. POLICY VIOLATIONS
Violations of University policies governing the use of University electronic mail services may result in restriction of access to University information technology resources. In addition, disciplinary action may be applicable under other University policies, guidelines, implementing procedures, or collective bargaining agreements, up to and including dismissal.

VIII. RESPONSIBILITY FOR POLICY

The Associate Vice President, Information Resources and Communications (IR&C) in the Office of the President is responsible for development, maintenance, and publication of this Policy.

IX. CAMPUS RESPONSIBILITY AND DISCRETION

Each campus shall develop, maintain, and publish specific procedures and practices that implement this Policy and communicate its provisions to campus users of University electronic mail services. The following are assigned to individual campus authority and discretion:

A. Each campus shall decide whether to publish its students' electronic mail addresses as directory information. An electronic mail address assigned by the University to a student is a student record, unless assigned in the student's capacity, if any, as an employee or agent of the University. In accordance with the policies and procedures in the University's "Policy Applying to the Disclosure of Information from Student Records" (Sections 130-134 of the Policies Applying to Campus Activities, Organizations, and Students), campuses are responsible for designating the categories of personally identifiable information about a student that are public. Individual students may, consistent with the above policy, request the campus not to make their email addresses public for other than educational purposes.

B. Each campus shall establish guidelines as to who may use campus electronic mail services, consistent with the provisions of Section VI. A of this Policy.

C. Each campus shall establish regulations and procedures on actions to be taken once an email user's affiliation with the campus is terminated. In particular, the campus may elect to: terminate the individual's email account, redirect electronic mail, or continue the account, subject to the provisions of Section VI. A of this Policy.

D. Each campus shall establish guidelines and procedures for:

1. Restriction of use of University email services pursuant to Section V. C of this Policy;

2. Authorization, notification, and recourse pursuant to Sections V. E and F of this Policy;

3. Response to requests for information from users concerning the back-up of electronic mail, pursuant to Section VI. B. 5 of this Policy; and

4. Any other provisions of this Policy for which procedures are not explicitly stated.

E. Each campus shall designate the appropriate Vice Chancellor to be responsible for the authorization of action pursuant to Sections V. C and E of this Policy. This authorization responsibility may not be further re-delegated.

F. Each campus shall establish appropriate notification procedures regarding this Policy to all email users, including positive acknowledgment by email users of receipt and understanding. Such notification and acknowledgment can be electronic to the extent that the email user's identity can be assured. It is recognized that it may take time to phase in such procedures; however, the lack of comprehensive procedures shall not, in the interim, invalidate the provisions and applicability of this Policy.
G. Each campus may establish its own procedures that further refine and conform with this Policy.

H. For purposes of this Section IX, the Office of the President shall be regarded as a campus with respect to its own internal operations, except that for this purpose Vice President shall replace Vice Chancellor in Sections V. C and E.

---

APPENDIX A - DEFINITIONS

**Computing Facility(ies):** Computing resources, services, and network systems such as computers and computer time, data processing or storage functions, computer systems and services, servers, networks, input/output and connecting devices, and related computer records, programs, software, and documentation.

**Electronic Mail System or Services:** Any messaging system that depends on computing facilities to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print computer records for purposes of asynchronous communication across computer network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic mail; or is implicitly used for such purposes, including services such as electronic bulletin boards, listservers, and newsgroups.

**University Email System or Services:** Electronic mail system or services owned or operated by the University or any of its sub-units.

**Email Record or Email:** Any or several electronic computer records or messages created, sent, forwarded, replied to, transmitted, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several email systems or services. This definition of email records applies equally to the contents of such records and to transactional information associated with such records, such as headers, summaries, addresses, and addressees. This Policy applies only to electronic mail in its electronic form. The Policy does not apply to printed copies of electronic mail.

**University Record:** A "public record" as defined in Business and Finance Bulletin RMP-8, Legal Requirements on Privacy of and Access to Information and the California Public Records Act. "Public records" include any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained (by the University) regardless of physical form or characteristics. [California Government Code Section 6252(d)]. With certain defined exceptions, such University records are subject to disclosure under the California Public Records Act.

Records held by students, including email, are not University records unless such records are pursuant to an employment or agent relationship the student has or has had with the University. This exemption does not, however, exclude student email from other aspects of this Policy, regardless of whether such email is a University record.

**University Email Record:** A University record in the form of an email record regardless of whether any of the computing facilities utilized to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print the email record are owned by the University. This implies that the location of the record, or the location of its creation or use, does not change its nature as: (i) a University email record for purposes of this or other University policy (see, however, Sections V. D and E), and (ii) having potential for disclosure under the California Public Records Act.

Until determined otherwise or unless it is clear from the context, any email record residing on university-owned computing facilities may be deemed to be a University email record for purposes of this Policy. This includes, for example, personal email (see Section VI. A. 8). Consistent, however, with the principles asserted in Section V. E. of least perusal and least action necessary and of legal compliance, the University must make a good faith a priori effort to distinguish University email records from personal and other email where relevant
to disclosures under the California Public Records Act and other laws, or for other applicable purposes of this Policy.

Use of University or other Email Services: To create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print email (with the aid of University email services). A (University) Email User is an individual who makes use of (University) email services.

Receipt of email prior to actual viewing is excluded from this definition of "use" to the extent that the recipient does not have advance knowledge of the contents of the email record.

Possession of Email: An individual is in "possession" of an email record, whether the original record or a copy or modification of the original record, when that individual has effective control over the location of its storage. Thus, an email record that resides on a computer server awaiting download to an addressee is deemed, for purposes of this Policy, to be in the possession of that addressee. Systems administrators and other operators of University email services are excluded from this definition of possession with regard to email not specifically created by or addressed to them.

Email users are not responsible for email in their possession when they have no knowledge of its existence or contents.

Holder of an Email Record or Email Holder: An email user who is in possession of a particular email record, regardless of whether that email user is the original creator or a recipient of the content of the record.

Substantiated Reason: Reliable evidence indicating that violation of law or policy probably has occurred, as distinguished from rumor, gossip, or other unreliable evidence.

APPENDIX B - REFERENCES

The following list identifies significant sources used as background in the preparation of this Policy, whether or not they are directly referenced by this Policy. It does not, however, include all federal and state laws and University policies that may apply to electronic mail. These policies and laws change from time to time, therefore users of this Policy are encouraged to refer to on-line versions of this and other University policies accessible on the Office of the President home page on the World Wide Web.

1. University Policies and Guidelines

   □ Business and Finance Bulletins:
   
   ■ A 56, Academic Support Unit Costing and Billing Guidelines
   ■ BUS 29, Management and Control of University Equipment
   ■ BUS-43, Materiel Management
   ■ BUS-65, Guidelines for University Mail Services
   ■ IS-3, Guidelines for Security of Computing Facilities
   ■ IS 6, Campus Communications Guidelines
   ■ RMP-1, University Records Management Program
   ■ RMP-2, University Records Disposition Program
   ■ RMP-7, Privacy of and Access to Information Responsibilities
   ■ RMP-8, Legal Requirements on Privacy of and Access to Information

   □ Personnel Manuals and Agreements:
   
   ■ Academic Personnel Manual
   ■ Personnel Policies for Staff Members
- Administrative and Professional Staff Program Personnel Policies
- Staff Personnel Policies
- Collective Bargaining Contracts (Memoranda of Understanding)

- Other Related Policies and Guidelines:
  - Campus Access Guidelines for Employee Organizations (Local Time, Place, and Manner Rules)
  - Policies Applying to Campus Activities, Organizations, and Students
  - Policy and Guidelines on the Reproduction of Copyrighted Materials for Teaching and Research
  - Policy on Copyright Ownership
  - University of California Records Disposition Schedules Manual

- State of California Statutes
  - State of California Education Code, Section 67100 et seq.
  - State of California Information Practices Act of 1977 (Civil Code Section 1798 et seq.)
  - State of California Public Records Act (Gov. Code Section 6250 et seq.)
  - State of California Penal Codes, Section 502

- Federal Statutes
  - Federal Family Educational Rights and Privacy Act of 1974,
  - Federal Privacy Act of 1974
  - Electronic Communications Privacy Act

---

Last updated August 1, 1996
APPENDIX B
UNIVERSITY OF CALIFORNIA
OFFICE OF THE PRESIDENT
ELECTRONIC MAIL POLICY

Reissued March 23, 1998
TABLE OF CONTENTS

I. INTRODUCTION .......................................................................................................................... 1
   Cautions.............................................................................................................................................. 1
II. PURPOSE .......................................................................................................................................... 2
III. DEFINITIONS ................................................................................................................................ 3
IV. SCOPE ............................................................................................................................................... 3
V. GENERAL PROVISIONS ............................................................................................................. 4
   A. Purpose ......................................................................................................................................... 4
   B. University Property ..................................................................................................................... 4
   C. Service Restrictions .................................................................................................................... 4
   D. Consent and Compliance ............................................................................................................ 5
   E. Restrictions on Access Without Consent .................................................................................. 5
   F. Recourse ..................................................................................................................................... 6
   G. Misuse....................................................................................................................................... 6
VI. SPECIFIC PROVISIONS .............................................................................................................. 6
   A. Allowable Use .......................................................................................................................... 6
      1. Purpose .......................................................................................................................... 6
      2. Users ............................................................................................................................... 6
      3. Non-Competition ................................................................................................................. 7
      4. Restrictions ....................................................................................................................... 7
      5. Representation .................................................................................................................... 7
      6. False Identity ..................................................................................................................... 7
      7. Interference ....................................................................................................................... 7
      8. Personal Use ..................................................................................................................... 7
   B. Security and Confidentiality ..................................................................................................... 8
   C. Archiving and Retention ......................................................................................................... 9
VII. POLICY VIOLATIONS .............................................................................................................. 10
VIII. RESPONSIBILITY FOR POLICY ............................................................................................. 10
IX. CAMPUS RESPONSIBILITIES & DISCRETION ........................................................................ 10
APPENDIX A, DEFINITIONS .............................................................................................................. 12
APPENDIX B, REFERENCES ............................................................................................................... 15
APPENDIX C, POLICIES RELATING TO NON-CONSENSUAL ACCESS ........................................ 17
I. INTRODUCTION

This Policy clarifies the applicability of law and of other University policies to electronic mail. It also defines new policy and procedures where existing policies do not specifically address issues particular to the use of electronic mail.

The University recognizes that principles of academic freedom and shared governance, freedom of speech, and privacy of information hold important implications for electronic mail and electronic mail services. The University affords electronic mail privacy protections comparable to that which it traditionally affords paper mail and telephone communications. This Policy reflects these firmly-held principles within the context of the University’s legal and other obligations.

The University encourages the use of electronic mail and respects the privacy of users. It does not routinely inspect, monitor, or disclose electronic mail without the holder’s (as defined in Appendix A, Definitions) consent. Nonetheless, subject to the requirements for authorization, notification, and other conditions specified in this Policy, the University may deny access to its electronic mail services and may inspect, monitor, or disclose electronic mail (i) when required by and consistent with law; (ii) when there is substantiated reason (as defined in Appendix A, Definitions) to believe that violations of law or of University policies listed in Appendix C have taken place; (iii) when there are compelling circumstances as defined in Appendix A; or (iv) under time-dependent, critical operational circumstances as defined in Appendix A, Definitions.

Cautions:
Users should be aware of the following:

1. Both the nature of electronic mail and the public character of the University's business (see Caution 2 below) make electronic mail less private than users may anticipate. For example, electronic mail intended for one person sometimes may be widely distributed because of the ease with which recipients can forward it to others. A reply to an electronic mail message posted on an electronic bulletin board or “listserver” intended only for the originator of the message may be distributed to all subscribers to the listserver. Furthermore, even after a user deletes an electronic mail record from a computer or electronic mail account it may persist on backup facilities, and thus be subject to disclosure under the provisions of Section V of this Policy. The University cannot routinely protect users against such eventualities.

2. Electronic mail, whether or not created or stored on University equipment, may constitute a University record (see Appendix A, Definitions) subject to disclosure under the California Public Records Act or other laws, or as a result of litigation. However, the University does not automatically comply with all requests for disclosure, but evaluates all such requests
against the precise provisions of the Act, other laws concerning disclosure and privacy, or other applicable law.

Users of University electronic mail services also should be aware that the California Public Records Act and other similar laws jeopardize the ability of the University to guarantee complete protection of personal electronic mail resident (see Section VI. A. 8) on University facilities.

The California Public Records Act does not, in general, apply to students except in their capacity, if any, as employees or agents of the University. This exemption does not, however, exclude student email from other aspects of this Policy.

3. The University, in general, cannot and does not wish to be the arbiter of the contents of electronic mail. Neither can the University, in general, protect users from receiving electronic mail they may find offensive. Members of the University community, however, are strongly encouraged to use the same personal and professional courtesies and considerations in electronic mail as they would in other forms of communication.

4. There is no guarantee, unless “authenticated” mail systems are in use, that electronic mail received was in fact sent by the purported sender, since it is relatively straightforward, although a violation of this Policy, for senders to disguise their identity. Furthermore, electronic mail that is forwarded may also be modified. Authentication technology is not widely and systematically in use at the University as of the date of this Policy. As with print documents, in case of doubt receivers of electronic mail messages should check with the purported sender to validate authorship or authenticity.

5. Encryption of electronic mail is another emerging technology that is not in widespread use as of the date of this Policy. This technology enables the encoding of electronic mail so that for all practical purposes it cannot be read by anyone who does not possess the right key. The answers to questions raised by the growing use of these technologies are not now sufficiently understood to warrant the formulation of University policy at this time. Users and operators of electronic mail facilities should be aware, however, that these technologies will become generally available and probably will be increasingly used by members of the community.

II. PURPOSE

The purpose of this Policy is to assure that:

A. The University community is informed about the applicability of policies and laws to electronic mail;

B. Electronic mail services are used in compliance with those policies and laws;
C. Users of electronic mail services are informed about how concepts of privacy and security apply to electronic mail; and

D. Disruptions to University electronic mail and other services and activities are minimized.

III. DEFINITIONS

The terms “electronic mail” and “email” are used interchangeably throughout this Policy.

The following terms used in this Policy are defined in Appendix A. Knowledge of these definitions is important to an understanding of this Policy:

- Computing Facility(ies)
- Electronic Mail Systems or Services
- University Email Systems or Services
- Email Record or Email
- University Record
- University Email Record
- Use of University or Other Email Services
- Possession of Email
- Holder of an Email Record or Email Holder
- Faculty
- Substantiated Reason
- Compelling Circumstances
- Emergency Circumstances
- Time-dependent, Critical, Operational Circumstances

IV. SCOPE

This Policy applies to:

- All electronic mail systems and services provided or owned by the University; and
- All users, holders, and uses of University email services; and
- All University email records in the possession of University employees or other email users of electronic mail services provided by the University.

Excluded from the foregoing are electronic mail services of Department of Energy Laboratories managed by the University, and email users of such electronic mail services who are employees and agents of those Laboratories.
This Policy applies only to electronic mail in its electronic form. The Policy does not apply to printed copies of electronic mail. Other University records management policies (see RMP series policies listed in Appendix B, References), however, do not distinguish among the media in which records are generated or stored. Electronic mail messages, therefore, in either their electronic or printed forms, are subject to those other policies, including provisions of those policies regarding retention and disclosure.

This Policy applies equally to transactional information (such as email headers, summaries, addresses, and addressees) associated with email records as it does to the contents of those records.

This Policy is effective immediately, with implementation guidelines to be effective July 1, 1998 (See Section IX).

V. GENERAL PROVISIONS

As noted in the Introduction, the University recognizes that principles of academic freedom, freedom of speech, and privacy of information hold important implications for electronic mail and electronic mail services. This Policy reflects these firmly-held principles within the context of the University’s legal and other obligations.

A. Purpose. In support of its threefold mission of instruction, research, and public service, the University encourages the use of University electronic mail services to share information, to improve communication, and to exchange ideas.

B. University Property. University electronic mail systems and services are University facilities as that term is used in other policies and guidelines. Any electronic mail address or account associated with the University, or any sub-unit of the University, assigned by the University to individuals, sub-units, or functions of the University, is the property of The Regents of the University of California.

C. Service Restrictions. Those who use University electronic mail services are expected to do so responsibly, that is, to comply with state and federal laws, with this and other policies and procedures of the University, and with normal standards of professional and personal courtesy and conduct. Access to University electronic mail services, when provided, is a privilege that may be wholly or partially restricted by the University without prior notice and without the consent of the email user when required by and consistent with law, when there is substantiated reason (as defined in Appendix A, Definitions) to believe that violations of policy or law have taken place, or, in exceptional cases, when required to meet time-dependent, critical operational needs. Such restriction is subject to established campuswide procedures or, in the absence of such procedures, to the approval of the appropriate campus Vice Chancellor or University Vice President.
D. **Consent and Compliance.** An email holder’s consent shall be sought by the University prior to any inspection, monitoring, or disclosure of University email records in the holder’s possession, except as provided for in Section V. E. University employees are, however, expected to comply with University requests for copies of email records in their possession that pertain to the administrative business of the University, or whose disclosure is required to comply with applicable laws, regardless of whether such records reside on a computer housed or owned by the University. Failure to comply with such requests can lead to the conditions of Section V. E.

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

When the contents of email must be inspected, monitored, or disclosed without the holder’s consent, the following shall apply:

1. **Authorization.** Except in emergency circumstances as defined in Appendix A, Definitions, and pursuant to Paragraph V.E.2, such actions must be authorized in advance and in writing by the responsible (see Section IX, Campus Responsibilities) campus Vice Chancellor or University Vice President. This authority may not be further re-delegated. Requests for such non-consensual access must be submitted in writing following procedures to be defined by each campus. University counsel’s advice shall be sought prior to authorization because of changing interpretations by the courts of laws affecting the privacy of electronic mail, and because of potential conflicts among different applicable laws. Where the inspection, monitoring, or disclosure of email held by faculty is involved, the advice of the Campus Academic Senate shall be sought in writing in advance, following procedures to be established by each campus. All such advice shall be given in a timely manner. Authorization shall be limited to the least perusal of contents and the least action necessary to resolve the situation.

2. **Emergency Circumstances.** In emergency circumstances as defined in Appendix A, Definitions, the least perusal of contents and the least action necessary to resolve the emergency may be taken immediately without authorization, but appropriate authorization must then be sought without delay following the procedures described in Section V. E. 1 above. If the action taken is not subsequently authorized, the responsible authority shall seek to have the situation restored as closely as possible to that which existed before action was taken.

3. **Notification.** In either case, the responsible authority or designee shall, at the earliest possible opportunity that is lawful and consistent with other University
4. **Compliance with Law.** Actions taken under Paragraphs 1. and 2. shall be in full compliance with the law and other applicable University policy, including laws and policies listed in Appendix B. This has particular significance for email residing on computers not owned or housed by the University. Advice of counsel always must be sought prior to any action taken under such circumstances. It also has particular significance for email whose content is protected under the Federal Family Educational Rights and Privacy Act of 1974, which applies equally to email as it does to print records.

F. **Recourse.** Procedures for the review and appeal of actions taken under Sections V. C, D, and E and under Section VII shall be implemented (or existing procedures adapted) by each campus to provide a mechanism for recourse to individuals who believe that actions taken by employees or agents of the University were in violation of this Policy.

G. **Misuse.** In general, both law and University policy prohibit the theft or other abuse of computing resources. Such prohibitions apply to electronic mail services and include (but are not limited to) unauthorized entry, use, transfer, and tampering with the accounts and files of others, and interference with the work of others and with other computing facilities. Under certain circumstances, the law contains provisions for felony offenses. Users of electronic mail are encouraged to familiarize themselves with these laws and policies (see Appendix B, References).

VI. **SPECIFIC PROVISIONS**

A. **Allowable Use**

In general, use of University electronic mail services is governed by policies that apply to the use of all University facilities. In particular, use of University electronic mail services is encouraged and is allowable subject to the following conditions:

1. **Purpose.** Electronic mail services are to be provided by University organizational units in support of the teaching, research, and public service mission of the University, and the administrative functions that support this mission.

2. **Users.** Users of University electronic mail services are to be limited primarily to University students, faculty, and staff for purposes that conform to the requirements of this Section.
3. **Non-Competition.** University electronic mail services shall not be provided in competition with commercial services to individuals or organizations outside the University.

4. **Restrictions.** University electronic mail services may not be used for: unlawful activities; commercial purposes not under the auspices of the University; personal financial gain (see applicable academic personnel policies); personal use inconsistent with Section VI. A. 8; or uses that violate other University policies or guidelines. The latter include, but are not limited to, policies and guidelines (see Appendix B, References) regarding intellectual property, or regarding sexual or other forms of harassment.

5. **Representation.** Electronic mail users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the University or any unit of the University unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing the University.

6. **False Identity.** University email users shall not employ a false identity. Email may, however, be sent anonymously provided this does not violate any law or this or any other University policy, and does not unreasonably interfere with the administrative business of the University.

7. **Interference.** University email services shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities, or unwarranted or unsolicited interference with others’ use of email or email systems.

8. **Personal Use.** University electronic mail services may be used for incidental personal purposes provided that, in addition to the foregoing constraints and conditions, such use does not: (i) directly or indirectly interfere with the University operation of computing facilities or electronic mail services; (ii) burden the University with noticeable incremental cost; or (iii) interfere with the email user’s employment or other obligations to the University. Email records arising from such personal use may, however, be subject to the presumption in Appendix A, Definition of a University Email Record, regarding personal and other email records. Email users should assess the implications of this presumption in their decision to use University electronic mail services for personal purposes.

---

1 An appropriate disclaimer is: "These statements are my own, not those of the University of California."

2 Such uses include, but are not limited to, the use of email services to: (i) send or forward email chain letters; (ii) "spam," that is, to exploit listservers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited email; and (iii) "letter-bomb," that is, to resend the same email repeatedly to one or more recipients to interfere with the recipient’s use of email.
B. Security and Confidentiality

1. The confidentiality of electronic mail cannot be assured. Such confidentiality may be compromised by applicability of law or policy, including this Policy, by unintended redistribution, or because of inadequacy of current technologies to protect against unauthorized access. Users, therefore, should exercise extreme caution in using email to communicate confidential or sensitive matters.

2. Business and Finance Bulletin RMP-8, Legal Requirements on Privacy of and Access to Information, prohibits University employees and others from “seeking out, using, or disclosing” without authorization “personal or confidential” information, and requires employees to take necessary precautions to protect the confidentiality of personal or confidential information encountered in the performance of their duties or otherwise. This prohibition applies to email records. In this Policy the terms “inspect, monitor, or disclose” are used within the meaning of “seek, use, or disclose” as defined in RMP-8.

3. Notwithstanding the previous paragraph, users should be aware that, during the performance of their duties, network and computer operations personnel and system administrators need from time to time to observe certain transactional addressing information to ensure proper functioning of University email services, and on these and other occasions may inadvertently see the contents of email messages. Except as provided elsewhere in this Policy, they are not permitted to see or read the contents intentionally; to read transactional information where not germane to the foregoing purpose; or disclose or otherwise use what they have seen. One exception, however, is that of systems personnel (such as “postmasters”) who may need to inspect email when re-routing or disposing of otherwise undeliverable email. This exception is limited to the least invasive level of inspection required to perform such duties. Furthermore, this exception does not exempt postmasters from the prohibition against disclosure of personal and confidential information of the previous paragraph, except insofar as such disclosure equates with good faith attempts to route the otherwise undeliverable email to the intended recipient. Re-routed mail normally should be accompanied by notification to the recipient that the email has been inspected for such purposes.

4. The University attempts to provide secure and reliable email services. Operators of University electronic mail services are expected to follow sound professional practices in providing for the security of electronic mail records, data, application programs, and system programs under their jurisdiction. Since such professional practices and protections are not foolproof, however, the security and confidentiality of electronic mail cannot be guaranteed. Furthermore, operators of email services have no control over the security of email that has been downloaded to a user’s computer. As a deterrent to potential intruders and to misuse of email, email users should employ whatever protections (such as passwords) are available to them.
5. Users of electronic mail services should be aware that even though the sender and recipient have discarded their copies of an electronic mail record, there may be back-up copies that can be retrieved. Systems may be "backed-up" on a routine or occasional basis to protect system reliability and integrity, and to prevent potential loss of data. The back-up process results in the copying of data onto storage media that may be retained for periods of time and in locations unknown to the originator or recipient of electronic mail. The practice and frequency of back-ups and the retention of back-up copies of email vary from system to system. Electronic mail users are encouraged to request information on the back-up practices followed by the operators of University electronic mail services, and such operators are required to provide such information upon request.

C. Archiving and Retention

University records management policies do not distinguish among media with regard to the definition of University records. As such, electronic mail records are subject to these policies. In particular, such records are subject to disposition schedules in the University of California Records Disposition Schedules Manual, which distinguishes among different categories of records, from the ephemeral to the archival.

The University does not maintain central or distributed electronic mail archives of all electronic mail sent or received. Electronic mail is normally backed up (see Section VI. B. 5), if at all, only to assure system integrity and reliability, not to provide for future retrieval, although back-ups may at times serve the latter purpose incidentally. Operators of University electronic mail services are not required by this Policy to retrieve email from such back-up facilities upon the holder’s request, although on occasion they may do so as a courtesy.

Email users should be aware that generally it is not possible to assure the longevity of electronic mail records for record-keeping purposes, in part because of the difficulty of guaranteeing that electronic mail can continue to be read in the face of changing formats and technologies and in part because of the changing nature of electronic mail systems. This becomes increasingly difficult as electronic mail encompasses more digital forms, such as embracing compound documents composed of digital voice, music, image, and video in addition to text. Furthermore, in the absence of the use of authentication systems (see Section I, Caution 4), it is difficult to guarantee that email documents have not been altered, intentionally or inadvertently.

Email users and those in possession of University records in the form of electronic mail are cautioned, therefore, to be prudent in their reliance on electronic mail for purposes of maintaining a lasting record. Sound business practice suggests that consideration be given to transferring (if possible) electronic mail to a more lasting medium/format, such as acid-free paper or microfilm, where long-term accessibility is an issue.
VII. POLICY VIOLATIONS

Violations of University policies governing the use of University electronic mail services may result in restriction of access to University information technology resources. In addition, disciplinary action, up to and including dismissal, may be applicable under other University policies, guidelines, implementing procedures, or collective bargaining agreements.

VIII. RESPONSIBILITY FOR POLICY

The Associate Vice President, Information Resources and Communications (IR&C) in the Office of the President is responsible for development and maintenance of this Policy for issuance by the President.

IX. CAMPUS RESPONSIBILITIES AND DISCRETION

Each Chancellor shall develop, maintain, and publish specific procedures and practices that implement this Policy and communicate its provisions to campus users of University electronic mail services. The following are assigned to individual campus authority and discretion:

A. Each Chancellor shall decide whether to publish students’ electronic mail addresses as directory information. An electronic mail address assigned by the University to a student is a student record, unless assigned in the student’s capacity, if any, as an employee or agent of the University. In accordance with the policies and procedures in the University’s “Policy Applying to the Disclosure of Information from Student Records” (Sections 130-134 of the Policies Applying to Campus Activities, Organizations, and Students), campuses are responsible for designating the categories of personally identifiable information about a student that are public. Individual students may, consistent with the above policy, request the campus not to make their email addresses public for other than educational purposes.

B. Each campus shall establish guidelines as to who may use campus electronic mail services, consistent with the provisions of Section VI. A of this Policy.

C. Each Chancellor shall establish regulations and procedures on actions to be taken once an email user’s affiliation with the campus is terminated. In particular, the campus may elect to terminate the individual’s email account, redirect electronic mail, or continue the account, subject to the provisions of Section VI. A of this Policy.

D. Each campus shall establish guidelines and procedures for:
1. Restriction of use of University email services pursuant to Section V. C of this Policy;

2. Authorization, advice, notification, and recourse pursuant to Sections V. E and F of this Policy;

3. Response to requests for information from users concerning the back-up of electronic mail, pursuant to Section VI. B. 5 of this Policy; and

4. Any other provisions of this Policy for which procedures are not explicitly stated.

E. Each Chancellor shall designate the appropriate Vice Chancellor to be responsible for the authorization of action pursuant to Sections V. C and E of this Policy. This authorization responsibility may not be further re-delegated.

F. Each campus shall establish appropriate notification procedures regarding this Policy to all email users. New users shall positively acknowledge receipt and understanding of the policy. Such notification and acknowledgment may be electronic to the extent that the email user's identity can be assured. It is recognized that it may not be possible to phase in such procedures immediately; however, the lack of comprehensive procedures shall not, in the interim, invalidate the provisions and applicability of this Policy.

G. Each campus may establish its own procedures that further refine and conform with this Policy.

H. For purposes of this Section IX, the Office of the President shall be regarded as a campus with respect to its own internal operations, except that for this purpose 'Vice President' shall replace 'Vice Chancellor' in Sections V. C and E.
APPENDIX A
DEFINITIONS

Computing Facility(ies): Computing resources, services, and network systems such as computers and computer time, data processing or storage functions, computer systems and services, servers, networks, input/output and connecting devices, and related computer records, programs, software, and documentation.

Electronic Mail Systems or Services: Any messaging system that depends on computing facilities to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print computer records for purposes of asynchronous communication across computer network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic mail or is implicitly used for such purposes, including services such as electronic bulletin boards, listservers, and newsgroups.

University Email Systems or Services: Electronic mail systems or services owned or operated by the University or any of its sub-units.

Email Record or Email: Any or several electronic computer records or messages created, sent, forwarded, replied to, transmitted, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several email systems or services. This definition of email records applies equally to the contents of such records and to transactional information associated with such records, such as headers, summaries, addresses, and addressees. This Policy applies only to electronic mail in its electronic form. The Policy does not apply to printed copies of electronic mail.

University Record: A “public record” as defined in Business and Finance Bulletin RMP-8, Legal Requirements on Privacy of and Access to Information and the California Public Records Act. “Public records” include any writing containing information relating to the conduct of the public’s business prepared, owned, used, or retained (by the University) regardless of physical form or characteristics. [California Government Code Section 6252(d)]. With certain defined exceptions, such University records are subject to disclosure under the California Public Records Act.

Records held by students, including email, are not University records unless such records are pursuant to an employment or agent relationship the student has or has had with the University. This exemption does not, however, exclude student email from other aspects of this Policy, regardless of whether such email is a University record.

University Email Record: A University Record in the form of an email record regardless of whether any of the computing facilities utilized to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print the email record are owned by the University. This implies that the location of the record, or the location of its creation or use, does not change its nature as: (i) a University email record for purposes of this or other University policy (see, however, Sections V. D and E), and (ii) having potential for disclosure under the California Public Records Act.
Until determined otherwise or unless it is clear from the context, any email record residing on university-owned computing facilities may be deemed to be a University email record for purposes of this Policy. This includes, for example, personal email (see Section VI. A. 8). Consistent, however, with the principles asserted in Section V. E. of least perusal and least action necessary and of legal compliance, the University must make a good faith a priori effort to distinguish University email records from personal and other email where relevant to disclosures under the California Public Records Act and other laws, or for other applicable purposes of this Policy.

**Use of University or Other Email Services:** To create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print email (with the aid of University email services). A (University) Email User is an individual who makes use of (University) email services.

Receipt of email prior to actual viewing is excluded from this definition of “use” to the extent that the recipient does not have advance knowledge of the contents of the email record.

**Possession of Email:** An individual is in “possession” of an email record, whether the original record or a copy or modification of the original record, when that individual has effective control over the location of its storage. Thus, an email record that resides on a computer server awaiting download to an addressee is deemed, for purposes of this Policy, to be in the possession of that addressee. Systems administrators and other operators of University email services are excluded from this definition of possession with regard to email not specifically created by or addressed to them.

Email users are not responsible for email in their possession when they have no knowledge of its existence or contents.

**Holder of an Email Record or Email Holder:** An email user who is in possession of a particular email record, regardless of whether that email user is the original creator or a recipient of the content of the record.

**Faculty:** A member of the faculty as defined by Academic Personnel Policy 110-4 (14).

**Substantiated Reason:** Reliable evidence indicating that violation of law or of policies listed in Appendix C probably has occurred, as distinguished from rumor, gossip, or other unreliable evidence.

**Compelling Circumstances:** Circumstances where failure to act may result in significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of University policies listed in Appendix C, or significant liability to the University or to members of the University community.

**Emergency Circumstances:** Circumstances where time is of the essence and where there is a high probability that delaying action would almost certainly result in compelling circumstances.
**Time-dependent and Critical Operational Circumstances:** Circumstances where failure to act could seriously hamper the ability of the University to function administratively or to meet its teaching obligations, but excluding circumstances pertaining to personal or professional activities, or to faculty research or matters of shared governance.
APPENDIX B
REFERENCES

The following list identifies significant sources used as background in the preparation of this Policy, whether or not they are directly referenced by this Policy. It does not, however, include all federal and state laws and University policies that may apply to electronic mail. These policies and laws change from time to time; therefore users of this Policy are encouraged to refer to on-line versions of this and other University policies accessible on the Office of the President home page on the World Wide Web.

University Policies and Guidelines

• Business and Finance Bulletins:

  A-56, Academic Support Unit Costing and Billing Guidelines
  BUS-29, Management and Control of University Equipment
  BUS-43, Materiel Management
  BUS-65, Guidelines for University Mail Services
  IS-3, Guidelines for Security of Computing Facilities
  IS-6, Campus Communications Guidelines
  RMP-1, University Records Management Program
  RMP-2, Records Disposition Program and Procedures
  RMP-7, Privacy of and Access to Information Responsibilities
  RMP-8, Legal Requirements on Privacy of and Access to Information

• Personnel Policies and Agreements:

  Academic Personnel Policy
  Personnel Policies for UC Staff Members (PPSM, current edition)
  Administrative and Professional Staff Program Personnel Policies
  Staff Personnel Policies
  Collective Bargaining Contracts (Memoranda of Understanding)

• Other Related Policies and Guidelines:

  Campus Access Guidelines for Employee Organizations (Local Time, Place, and Manner Rules)
  Policies Applying to Campus Activities, Organizations, and Students
  Policy and Guidelines on the Reproduction of Copyrighted Materials for Teaching and Research
  Policy on Copyright Ownership
  University of California Records Disposition Schedules Manual
  University Policy on Integrity in Research
State of California Statutes

State of California Education Code, Section 67100 et seq.
State of California Information Practices Act of 1977 (Civil Code Section 1798 et seq.)
State of California Public Records Act (Gov. Code Section 6250 et seq.)
State of California Penal Code, Section 502

Federal Statutes

Federal Family Educational Rights and Privacy Act of 1974
Federal Privacy Act of 1974
Electronic Communications Privacy Act of 1986
This University Electronic Mail Policy references circumstances where access to electronic mail may occur without the prior consent of the holder (see I. Introduction and Section V.E). Following is the list of University policies that may trigger such non-consensual access following procedures defined in Section V.E.2.

1. Policies governing sexual or other forms of harassment, specifically: Section APM-035, Appendix A of the Faculty Code of Conduct; Personnel Policies for UC Staff Members; Administrative and Professional Staff Program Personnel Policies, Sections 112.1 and 112.2; Staff Personnel Policies, Section 200.2. (For exclusively represented employees in units where initial collective bargaining agreements are under negotiation, applicable personnel policies continue to govern until an agreement is concluded.) Sexual harassment by students is covered by item 6 below.

2. Certain portions of policies governing access to University records, specifically RMP-1, Section III; RMP-8, Section VIIG; and RMP-8, Exhibit D.

3. The Academic Personnel Manual, APM-015, Section II, Part II, limited to those parts headed Unacceptable Faculty Conduct, and the University Policy on Integrity in Research.

4. University of California Personnel Policies for Staff Members, Administrative and Professional Staff Program Personnel Policies and Staff Personnel Policies. (For exclusively represented employees in units where initial collective bargaining agreements are under negotiation, applicable personnel policies continue to govern until an agreement is concluded.)

5. All collective bargaining agreements and memoranda of understanding.

6. Section 102, governing student conduct, of the policy entitled “Policies Applying to Campus Activities, Organizations, and Students”.

7. Sections V and VI of this Electronic Mail Policy.

Violations of other policies can normally be detected and investigated without requiring non-consensual access to electronic mail. However, on occasion attention to possible policy violations is brought about because of the receipt by others of electronic mail. Electronic mail, however can be forged; the true identity of the sender can be masked; and the apparent sender may deny authorship of the electronic mail. In such circumstances and provided there is substantiated reason (as defined in Appendix A, Definitions) that points to the identity of the sender, non-consensual access to the purported sender’s electronic mail may be authorized following the procedures defined in Section V.2, but only to the least extent necessary for verifying unambiguously the identity of the sender, and only for major violations of the following policies:
• Business and Finance Bulletin A-56, Section IV-H, governing sales of goods or services outside the University.

• Business and Finance Bulletin BUS-29, Section N, governing use of University materiel or property.

• Business and Finance Bulletin BUS-43, Part 3, Section X-A, governing use of University credit, purchasing power, or facilities.

• Policies Applying to Campus Activities, Organizations, and Students, Section 42.40, governing use of University properties for commercial purposes and personal financial gain.

• Business and Finance Bulletin BUS-65, Section VII, governing provision of University mailing lists to others.

• Policy and Guidelines on the Reproduction of Copyrighted Materials for Teaching and Research.

• Campus Access Guidelines for Employee Organizations.

**Posting and Authority to Change**

Because University policies are subject to change, this list may change from time to time. The authoritative list at any time will be posted under the listings of University policies posted on the World Wide Web. Authority to change this list rests with the President of the University acting, where policies affecting faculty are concerned, with the advice of the Academic Senate.
A. UC Climate Assessment for Learning, Living, and Working
Christine Littleton, Vice Provost, Diversity & Faculty Development (55 min)
Susan Drange Lee, Director, Faculty Diversity & Development
UC President Yudof has commissioned a systemwide survey of all UC students, faculty and
staff to better understand the University climate, in order to be able to improve it. The survey
is expected to be implemented during Fall/Winter 2012-13.
ACTION: Advise Chancellor Block, EVC and Provost Waugh and VP Littleton on the
operational privacy principles that should guide the conduct of the survey.

B. Laptop anti-theft software
Matt Ellis, Manager, CSO Programs, UCLA Police (20 min)
The UCLA Police and Insurance and Risk Management have purchased Frontdoor Software
licenses for UCLA students, faculty and staff, initially for use on personally owned devices. It
has a good track record in helping recover stolen or lost laptops.
ACTION: Advise the Common Systems Group on the operational privacy principles that
should guide use of this software on University-owned laptops.

C. UC Privacy and Information Security Initiative: Governance
Kent Wada and Marti Arvin (15 min)
A proposed governance model for privacy and information security, at both the systemwide
and campus levels, is being discussed as part of the UC initiative.
ACTION: Consider the implications of this model in light of UCLA’s structure to provide input
to the systemwide initiative and to campus governance.

D. UCLA Privacy Board and Its Role in Privacy “Operations”
Jim Davis (30 min)
ACTION: Consider an increased role for the Privacy Board, including, potentially:
1. Providing directional and strategic guidance on privacy to the Oversight Committee on
   Audit, IT Governance, Compliance and Controls via EVC and Provost Waugh and
   VC-Legal Affairs and Campus Ethics and Compliance Officer Reed.
2. Responding to new, strategic privacy situations by employing the proposed UC Privacy
   Framework: UC privacy principles and the balancing test.
3. Building the portfolio of case situations.
Marti Arvin, Chief Compliance Officer, Medical Sciences
Stuart Biegel, Education Faculty & Law Faculty
Amy Blum, Senior Campus Counsel
Christine Borgman, Professor and Presidential Chair, Information Studies
Alfonso Cardenas, Professor, Computer Science
Dana Cuff, Professor and Vice Chair, Architecture and Urban Planning
Michael Curry, Professor, Geography
Jim Davis, Vice Provost, Information Technology and
Chief Academic Technology Officer (chair)
Sharon Friend, Director,
Office of Human Research Protection Program
Maryann Jacobi Gray, Assistant Provost,
Office of the Executive Vice Chancellor and Provost
David Harmon, Director, Financial Management
Programs, Corporate Financial Services
Leah Lievrouw, Professor, Information Studies
Rafail Ostrovsky, Professor, Computer Science
Dinesh Shadrach, Graduate Student Representative, Anderson School
Gary Strong, University Librarian
Burton Swanson, Professor, Anderson School
Kent Wada, Director, IT Strategic and Privacy Policy
TBD – Faculty member
TBD – Undergraduate Student Representative

Resources
Ross Bollens, Director, IT Security
Claudia Luther, Senior Media Relations Representative
APPENDIX D
Campus Position Statement on Privacy

The University community fosters academic freedom through promoting the right to teach, the right to learn, and the right to inquire. Academic freedom is most vibrant where individuals have autonomy; where their inquiry is free because it is given adequate space for experimentation.

New technologies can enable greater experimentation in ideas; they can also constrain free inquiry by collecting personal information and by making permanent records of intellectual exploration. In order to maintain robust academic freedom in light of greater personal information collection and storage, the Privacy Board has drafted this policy to promote privacy and individuals' autonomy.

The Privacy Board has identified five guidelines that are central to upholding privacy rights in information systems. These guidelines should inform the creation and modification of systems with information that can identify individuals:

- **Education.** The University should apply the privacy guidelines by educating the community and promoting knowledge of appropriate protections for personal information. The University should continue to take special efforts in educating members of the community who have access to personal information of privacy laws and regulations for use and disclosure of data.

- **Transparency.** Transparency in information systems promotes accountability, informs individuals of their rights and responsibilities, and allows individuals to take more enlightened decisions when disclosing or using data. In furtherance of its educational role, the University should inform individuals of the personal information collected and how it is used to perform official functions.

Where possible, and without creating undue bureaucracy, the University should strive to disclose the following aspects of personal information systems. These disclosures, drawn from the Organization of Economic Cooperation and Development, seek to balance the rights and responsibilities of data collectors and individuals by establishing "Fair Information Practices:"

- What information is collected.
- Why it is collected.
- Whether the collection is mandatory or voluntary.
- How long it is kept.
- Who has access to the information.
- The purposes for which the information can be used.

Position Statement Privacy 10/10/06
• What security safeguards are in place to protect the information.
• Who is responsible to address questions or complaints concerning the system.

Privacy-Friendly Design. The University should encourage the development of systems that deliver services or perform functions without the collection of personal information. Where possible, the University should allow individuals to decide whether or not to enroll in systems that collect personal information. Information systems should be designed consciously to avoid creating opportunities for information to be reused for purposes incompatible with the purpose of its collection, to avoid creating new surveillance opportunities, and to avoid the persistent maintenance of personal information.

Accountability and Fairness. There must be processes in place to ensure fairness where important decisions are made based on personal data. There should be recourse for members of the University community who desire to challenge a determination based on personal information.

Sustainability and Operational Necessity. The University performs myriad functions in addition to education and research, including providing housing, health care, communications, and transportation. Many of these functions require the collection of personal information. These guidelines should be applied in a reasonable manner so as to promote operational efficiency while striving to design systems that are sensitive to privacy risks.
Many privacy statements developed by colleges and universities adopt an e-commerce tone ("The University has adopted this privacy policy in order to inform you of?"). Because the Privacy Board indicated that it desired to make an intense statement, I recommend adopting a broader, principled tone. A Campus Position Statement should begin with an explanation of how privacy rights are grounded in academic freedom. It should explain how new technologies relate to academic freedom (explicitly enumerating the freedom to teach, to learn, and to inquire) and other University values. It should recognize that intellectual freedom could be limited in an environment where individuals' actions are under surveillance.

It should also explain that there is a tension between openness and privacy, one that may be mitigated by focusing efforts on protecting personal information while not hindering research or the freedom to publish. A narrative introduction could be used, or a series of "whereas" clauses stating findings could introduce the Position Statement.

Members of the Privacy Board discussed (at least) nine values that should be reflected in a Campus Position Statement. Some have aspects that overlap with each other, such as the importance of education about privacy issues and values of transparency. The nine values are:

1) Education. Members of the Privacy Board emphasized that the Campus Position Statement is an opportunity to educate the community on privacy issues. Attention must be paid to how the University's pedagogical role can inform the campus of privacy risks and how the risks can be addressed.

2) Transparency. Members of the Privacy Board emphasized the importance of "making the invisible become visible." More transparency will promote accountability, inform individuals, and allow them to take more enlightened decisions. A significant challenge remains: how can the University promote transparency in such a way that it does not cause members of the community to become apathetic, or otherwise feel that nothing can be done to solve privacy problems? A Campus Position Statement should make a strong commitment to ensuring that systems that collect personal information fully disclose:

a. What information is collected.
b. Why it is collected.
c. Whether the collection is mandatory or voluntary.
d. How long it is kept.
e. Who has access to the information.
f. The purposes for which the information can be used.
g. What security safeguards are in place to protect the information.
h. Who is responsible to address questions or complaints concerning the system.

3) Voluntary Participation. Members of the Privacy Board thought it important to determine whether individuals must enroll or otherwise participate in systems with privacy implications. A Campus Position Statement may encourage administrators to create systems that allow use of services without collection of personal information.

4) Changing norms and emerging technologies. A Campus Position Statement must recognize that privacy norms will change with time. In addition, technologies will enable new forms of surveillance and possibly, new protections for privacy.

5) The relationship with law enforcement. A Campus Position Statement should address University policy towards CALEA and the PATRIOT Act. Provisions would emphasize recognizing the risks of data collection and persistence, and perhaps urge creators of systems to limit data collection and retention.

6) Fairness and due process. A Campus Position Statement should emphasize that there must be processes in place to ensure fairness where important decisions are made based on personal data. There should be recourse for members of the University community who desire to challenge a determination based on personal information.

7) Sustainability. A Campus Position Statement must be well-vetted and general enough to be followed by the University community. It should be vigorous and ambitious without being impractical. It should be written in technology-neutral language to accommodate emerging technologies.

8) Accountability. The Privacy Board expressed interest in an ombudsperson position for privacy. Such a person would be tasked with receiving complaints concerning information systems, and establishing procedures to help individuals understand how to grieve.

9) Definitions. There should be agreement concerning the scope of the Campus Privacy Statement. Should it apply to systems that collect personally identifiable information? Or is that too narrow (do CCTV cameras collect personally identifiable information)?

Technologies Creating Challenges

In a typical enterprise-wide privacy inquiry, one would begin by performing a privacy audit that identified all systems containing personally-identifiable information. This first, complicated step would be followed by an assessment of privacy and security risks, the creation of reasonable procedures to mitigate these risks, and continued testing and training to ensure that the mitigation program was effective. Such a task would require intense time and financial commitments. As an alternative to a campus-wide privacy audit, the Privacy Board should consider performing an audit of individual systems that present privacy risks. These include:
1) External campus directory. Are students aware that their personal information included in directories based on an opt-out model? What information should be published in a directory? Are there ways of limiting directory use to certain, educationally-related functions?

2) Bruincard. Many questions surround the practices governing the principal identity card used at UCLA. What vendor actually provides the cards and hardware? What data are encoded on the card? Are there adequate audit trails to prevent personal use or other misuses of this data? When using the card, what information is logged? For instance, if a student is using the card to enter the gymnasium, is the identity of the student logged, or just the fact that a student with gymnasium privileges has entered? How long is data kept?

3) Closed-Circuit Television (CCTV). Cameras are proliferating around campus. Some may be operated for security reasons, others for research purposes. Are there campus-wide policies for installing CCTV? May these cameras be hidden? Is the University certain that audio is not being collected (which is illegal under state and federal wiretapping law)? What happens to the information collected by these cameras? How long is it kept? Who has access, and for what purposes?

4) Students' use of social networking systems. Social networking systems pose three serious risks: first, employers may use information submitted to such services in employment determinations. Students have not always been sensitive to this risk. Second, the rising popularity of location-based systems introduces the risk that individuals could be stalked. Third, students are self-reporting illegal behavior, behavior that violates university rules, and risk taking behavior. To what extent should the university monitor or investigate these disclosures? Does the University's in loco parentis role justify some intervention? If so, how can the University act without limiting students' expressive rights?

5) Background checks for employees. Federal and state law regulate the performance and scope of background checks. But in a University setting, should there be greater controls on the practice? Should the University extend more "social forgiveness" to individuals previously arrested or convicted of crimes than traditional employers?

6) Emerging technologies. RFID is increasingly used in identity systems. VOIP technology is replacing traditional phone systems. How will the University address the privacy risks arising from this and other technologies?
REFERENCES


Gayle, W., & Vermillion, E. (2001, July 29). Information Technology Infrastructure At The University of California. UCSF Information Technology Services Department and Budget & Resource Management Department.


Peer-to-Peer Piracy (P2P) on University Campuses: Hearing before the Subcommittee on Courts, the Internet and Intellectual Property Committee on the Judiciary, 108th Cong. 17 (2004) (testimony of James F. Davis).


