UCLA Statement on Privacy and Data Protection[1]

Prelude

The Advisory Board on Privacy and Data Protection is an advisory board to the Executive Vice Chancellor. It is charged with articulating an institutional position reflecting the campus's values and cultural expectations to address the challenging issues of balancing privacy and data protection faced by the campus community.

This Statement articulates principles and provides guidance for attaining the principles when complying with University and campus policy on privacy and data protection.[2] However, the Statement is not policy itself and does not confer nor abrogate any rights or privileges.

Table of Contents

[1] The Board would like to express its appreciation to Chris Jay Hoofnagle, now with the Berkeley Center for Law & Technology, for his work in framing this statement.
[2] This Statement does not speak to whistleblower policies or issues.

Statement

Individual privacy one of the values strongly supported by UCLA. It is a fundamental human right and plays an important role in human dignity, put by U.S. Supreme Court Justice Louis Brandeis as "the right to be let alone … the right most valued by civilized men"[3].

Privacy is an underpinning of academic freedom, upon which the mission of the University is dependent. Academic freedom[4] is 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.

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

- ensuring an appropriate level of privacy through its policies and practices, even as interpretations of privacy change over time;
- nurturing an environment of openness and creativity for teaching and research;
- honoring its obligation as a public institution to remain transparent, accountable and operationally effective; and
- safeguarding confidential information and assets for which it is a steward.

The Advisory Board on Privacy and Data Protection is the campus nexus for the ongoing discussion about appropriate balance in the context of an ever evolving societal, legal and technological climate.

Principles of Fair Information Practices

The following principles, drawn from the Organisation for Economic Co-operation and Development[5], help uphold privacy rights. They seek to balance the rights and responsibilities of data collectors and individuals by establishing a code of fair information practices. UCLA strives to align with these principles in its policies and implement these practices in its information systems[6].

1. *Transparency*. Transparency promotes accountability, informs individuals of their rights and responsibilities and allows individuals to make more enlightened decisions when disclosing or using data. In furtherance of its educational role, the campus should inform individuals of the personal information collected and how that information is used to perform official

[3] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* IV, no. 5 (December 1890).
[4] American Council on Education, "Statement on Academic Rights and Responsibilities," (2005).
[5] http://oecd.org/
[6] Examples of information systems include Registrar, BruinCard, library records and personnel records.

functions. Where possible, and without creating undue bureaucracy, the campus should strive to disclose the following aspects of personal information systems:

- Information sought
  a. What information is being collected.
  b. For what purpose it is being collected and the resulting benefit.
  c. Whether the collection is mandatory or voluntary.
  d. How long the information is kept.
  e. In what form it is kept, including documentation.
  f. The purpose(s) for which the information can be used.
- Stewardship
  g. Who is the steward of the data and has responsibility for addressing questions or complaints concerning the system or its content.
  h. Who has access to the information and by what means.[7]
  i. What security safeguards are in place to protect the information.[8]

2. *Privacy-Friendly Design*. The campus should encourage the development of information systems that deliver services or perform functions without the collection of personal information. Where possible, the campus should allow individuals to decide whether 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.
3. *Accountability and Fairness*. There must be processes in place to ensure fairness where important decisions are made based on personal data. There should be a mechanism for recourse for individuals who desire to challenge a determination based on personal information.
4. *Sustainability and Operational Necessity*. The campus 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 principles should be applied in a reasonable manner so as to promote operational effectiveness (including appropriate security safeguards) while striving to design systems that are sensitive to privacy risks.

[7] Only in general terms, without reference to specifics that could help an ill-intentioned individual inappropriately gain access to information.
[8] Again, only in general terms, without reference to specifics that could help an ill-intentioned individual inappropriately gain access to information.

Appendix A. Guidance for Attainment

The following sections give guidance for attaining the principles and for achieving an appropriate balance between privacy and compliance with applicable policies.

Privacy of Electronic Communications

This section is primarily applicable to the administration of networks, email servers and systems.

The University of California is governed by its Electronic Communications Policy (ECP) with respect to privacy of electronic communications. It articulates a bright-line threshold for protecting individual privacy: "The University does not examine or disclose electronic communications records without the holder's consent."[9] A high bar is set for overriding this protection ("non-consensual access procedure"[10]), which can occur only in specified circumstances[11] and which requires a multi-level review, including high-level review through the approval of the appropriate administrator at the minimum level of Vice Chancellor.[12]

Security, privacy, and other values and obligations must be appropriately balanced as articulated in the Statement. The following guidance can be applied to help resolve conflicts between values and/or varying interests.

1. Employ standard technical practices to ensure the security, reliability and integrity of electronic information systems, services and data. These practices include the routine monitoring of the network by automated means.
2. Do not allow security practices to be used for surveillance, or the monitoring of individual behavior.[13] If surveillance is required, appropriate guidance shall be sought and either the provisions for non-consensual access in the ECP followed or other legal requirements satisfied.
3. Do not "lock down" access so tightly that security becomes a barrier to collaboration or productivity. The appropriate balance between security risk and functionality must be considered.
4. Consistent with the ECP, do not intentionally search electronic communications for violations of law or policy. Do act to assure that

[9] UC ECP, Section IV.A Privacy and Confidentiality, Introduction.
http://www.ucop.edu/ucophome/policies/ec/html/pp081805ecp.html#A%20PRIVACY
[10] UC ECP, Section IV.B Access Without Consent.
http://www.ucop.edu/ucophome/policies/ec/html/pp081805ecp.html#B%20PRIVACY
[11] UC ECP, Section IV.B Access Without Consent: "(i) when required by and consistent with law; (ii) when there is substantiated reason […]to believe that violations of law or of University policies […]; (iii) when there are compelling circumstances […]; or (iv) under time-dependent, critical operational circumstances […]."
http://www.ucop.edu/ucophome/policies/ec/html/pp081805ecp.html#B%20PRIVACY
[12] UC ECP, Section IV.B Access Without Consent.
http://www.ucop.edu/ucophome/policies/ec/html/pp081805ecp.html#B%20PRIVACY
[13] However, also refer to the text on audit trails and other means for effecting due diligence in complying with legal or regulatory requirements in the section Protection of Confidential Information.

suspected, inadvertently discovered and reported violations are promptly and properly handled. If non-consensual access is required to do so, the ECP's procedure for such access must be followed.[12]

5. Avoid making judgments based on value of content (e.g., whether access to certain web sites is appropriate), as most a priori prohibitions on access to content are considered censorship.
6. Consult with the appropriate campus official(s) when conflicts arise between privacy and other policies or legal obligations (e.g., sexual harassment policies or human subjects protection).
7. Situations requiring emergency access should follow the specific procedure defined in the ECP for this purpose.[14]

Protection of Confidential Information

This section is primarily applicable to data stewards and to those administering or developing databases or other information systems and networks.

The University is the steward for the confidential information it requires to fulfill its missions and operations. To safeguard such information, the University employs practices that ensure confidentiality, foster clear accountability, increase the effectiveness of data administration and minimize legal exposure and liability.[15,16]

In order to effect due diligence in complying with legal requirements and to be good stewards of the public trust, appropriate controls must be implemented in systems and services containing confidential information. For research and clinical trials involving human subjects, approval by the Institutional Review Board[17] is Federally mandated. More generally, controls can take many forms, including administrative (e.g., background checks), physical (e.g., access to devices) or technical.

Technical controls include:

- Use of encryption technology[18] as generally required for Personal Information[19].
- Limiting access to specific data, systems or network content to only those who legitimately require access.

---

[14] UC ECP, Section IV.B.2. Emergency Circumstances.
http://ucop.edu/ucophome/policies/ec/html/pp081805ecp.html#B%20PRIVACY
[15] UC Business and Finance Bulletin IS-3 Electronic Information Security.
http://www.ucop.edu/ucophome/policies/bfb/is3.pdf
[16] UCLA Policy 404, Protection of Electronically Stored Personal Information.
http://www.adminpolicies.ucla.edu/app/Default.aspx?&id=404
[17] http://oprs.ucla.edu/human/about-IRBs
[18] UCLA Policy 404, Protection of Electronically Stored Personal Information, Section IV.A Campuswide Standards for Electronically Storing Personal Information.
http://www.adminpolicies.ucla.edu/app/Default.aspx?&id=404
[19] Defined by UCLA Policy 404 as an individual's first name or first initial, and last name, in combination with any one or more of the following: (1) Social Security number, (2) driver's license number or California identification card number, (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account, (4) medical information, and (5) health insurance information.

- The maintenance of an audit trail logging access to specific data, systems or network content (e.g., a clinical patient system) in order to permit the identification of potential wrongdoers.[20]
- Limiting access to network content or services not required for the intended purpose of the network, system or unit to minimize risk (e.g., prohibiting peer-to-peer protocols on a payroll network where there is no business or academic need for such tools — at present).

Use of controls such as audit trails and the limitation on access to specific network content or services can be necessary to effect due diligence in complying with legal or regulatory requirements.[21] Unless stipulated by law, however, such controls should be carefully considered so as to avoid violating the UC Electronic Communications Policy. Regardless, the ECP does require a minimization approach: only as much intrusive security as is appropriate in any given circumstance should be used and no more.[22]

Use of these technical controls does not abrogate other provisions of the ECP. For example, logging access to a specific system containing personally identifiable information does not mean a supervisor can look at an employee's email without his or her consent; or absent consent, going through the Policy's non-consensual access procedure.[12]

Legally Required Disclosures

The University is often required to disclose information it may not routinely make public: for example, when in receipt of a subpoena, during litigation or when a California Public Records Act (PRA) request is made. UCLA has existing policies and procedures that speak to these circumstances.[23,24,25] There are also requests made under the aegis of national security, which should always be referred to Campus or University Counsel.

It is important to be mindful that much information held or created by the University is subject to disclosure under the PRA to help ensure transparency and accountability for public institutions. For example, current salaries (as employees of a public institution) and routine email communications generally fall under this provision, though most personally identifiable information does not.

---

[20] UC Business and Finance Bulletin IS-3 Electronic Information Security, Appendix D, Log Management. http://www.ucop.edu/ucophome/policies/bfb/is3.pdf
[21] UC ECP, Section V, Security. http://www.ucop.edu/ucophome/policies/ec/html/pp081805ecp.html#SECURITY
[22] UC ECP, Section V.B, Security Practices: "Network traffic may be inspected to confirm malicious or unauthorized activity that may harm the campus network or devices connected to the network. Such activity shall be limited to the least perusal of contents required to resolve the situation." http://www.ucop.edu/ucophome/policies/ec/html/pp081805ecp.html#B%20SECURITY
[23] UCLA Procedure 120.1: Producing Records Under Subpoena Duces Tecum and Deposition Subpoenas. http://www.adminpolicies.ucla.edu/app/Default.aspx?&id=120-1
[24] UCLA Practices for Preservation of Electronically Stored Information [ESI]. http://www.campuscounsel.ucla.edu/documents/UCLA%20PRACTICES%20FOR%20ESI.pdf
[25] UCLA Policy 603: Privacy of and Access to Information (Legal Requirements). http://www.adminpolicies.ucla.edu/app/Default.aspx?&id=603

Specific computer security sensitive information – information that could directly assist malicious individuals in attacking UCLA applications, systems and networks – is not subject to an express statutory exemption, but is protected under a balance of interest rule. Thus when information relating directly to the security of systems is communicated, it should be identified as such with the label "Confidential: Computer Security Sensitive Information". This flags material for careful examination by campus attorneys when a PRA covers such information. It also makes it clear to anyone else seeing such information that extra care expected. Only the truly sensitive information should be so labeled.

Considerations for Individuals

An important rule of thumb is to avoid putting in an email anything you would prefer not end up as a headline in the newspaper. While incidental personal use of electronic resources is permitted[26], any individual concerned about individual privacy unrelated to University activities should use a separate commercial account for non-University related electronic records and communications.

Conversely, the convenience of free or low-cost external email 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.[27] Each individual must take responsibility when making decisions about when it is and is not acceptable to use these free/low cost services.

All legal and University policy requirements apply to all University records, whether on UC or non-UC systems.

Under no circumstances should confidential or restricted data[28] be used with services for which UC has not negotiated an agreement through the regular campus or University process.

[26] UC ECP, Section III.D.8, Personal Use.
http://ucop.edu/ucophome/policies/ec/html/pp081805ecp.html#D%20ALLOW

[27] Guidance on making informed decisions in this area is being developed. In the interim, such guidance from the University of California, Santa Cruz, provides excellent information on the use of free cloud services: http://its.ucsc.edu/security/policies/free.php.

[28] UC BFB IS-2 Inventory, Classification, and Release of University Electronic Information, Appendix A, Definitions.
http://ucop.edu/ucophome/policies/bfb/is2.pdf

Appendix B. Scenarios