New Models of Privacy for the University

Christine L. Borgman, Kent Wada, and James F. Davis[1], UCLA

To appear in:
Visions of Privacy in the Modern Age

Editors: Marc Rotenberg and Jeramie Scott

Electronic Privacy Information Center, Washington, DC, 2014

Introduction

Today's research universities face a plethora of competing challenges in the privacy arena. They aspire to provide welcoming spaces that encourage their communities to explore and to exchange new ideas. They are stewards of sensitive data collected by and about their communities, such as human subjects records, student records, and health information. The information resources held by research universities are valued in different ways, whether scholarly, operational, reputational, or commercial. Content may be open access, proprietary, or subject to ethical, regulatory, or licensing constraints. In all of these arenas, universities attempt to balance opportunity, obligations, impact, appropriate use, reputation, ethics, integrity, and institutional culture.

Universities are uniquely concerned with academic freedom, because "the common good depends upon the free search for truth and its free exposition" ("Academic Freedom," 2014). Faculty and students alike must be able to conduct their research, within accepted guidelines,

---

[1] The three authors are members of the UCLA Privacy and Data Protection Board and were members of the University of California Privacy and Information Security Committee. Christine L. Borgman is Professor and Presidential Chair in Information Studies at UCLA and a member of the EPIC Board of Directors. Kent Wada is UCLA Chief Privacy Officer. James F. Davis is Vice Provost for Information Technology & Chief Academic Technology Officer at UCLA. This article reflects the work of the UC Privacy and Information Security Steering Committee and Working Group, whose many names are listed on the final report.

without exposing their data prematurely. These freedoms are balanced with open records laws, open access policies for journal publication, and the requirements of funding agencies and journals to release data that are subject to peer review. Similarly, the needs of competing stakeholders often must be balanced: public-private partnerships, intellectual property regimes, open government, commercialization, and so on. Whereas privacy underpins an ethical and respectful environment for the entire university community, rarely do universities take a holistic approach to privacy, information security, and data governance. The time is nigh to do so, and the University of California has developed a proactive model that can be applied to other universities and institutions of higher learning.

The University of California, which is the largest public research university in the U.S., with ten campuses, five academic medical centers, three national laboratories, and more than 233,000 students and 190,000 faculty and staff, faces all of these privacy issues and more. In June of 2010, Mark Yudof, then President of the University of California, launched the Privacy and Information Security Initiative, charging the Steering Committee and Working Group to perform a comprehensive review of the university's current privacy and information security policy framework and to make recommendations about how the university should address near-term policy issues and longer-term governance issues. The committee consisted of a broad cross section of functional areas within the university and included representation from faculty, staff, and students. EPIC was among the groups consulted as part of the committee's research and deliberations. The final report, released January 2013, includes a UC Statement of Privacy Values and Privacy Principles, several recommendations, and an implementation timeline ("Privacy and Information Security Initiative, Final Report," 2014). The report was accepted, with minor modifications, and is now being implemented system wide (Lucas, Vacca, & Yudof, 2013).

The UC report makes several important contributions to debates about privacy and information security in higher education. One is to take a proactive, rather than a responsive or defensive approach, to privacy and information security. A second is to establish a framework of values and principles on which policy can be based. Third is to establish criteria for balancing the interests of stakeholders. Fourth is to establish a governance model that incorporates academic and administrative interests in decision-making and policy development.

The report presumes that technology, social norms, and policy evolve at differential rates. Ubiquitous access to, and creation of, information via mobile devices, social media, and virtual environments intersect with "real life" in unexpected ways, many of them privacy-related. By establishing a holistic framework for privacy and information security in universities, the report offers a vocabulary for thinking about privacy and information security. These concepts are placed in the constellation of university values and legal, policy, and administrative obligations.

Privacy and Information Security

A considerable portion of the two years of deliberations for the Initiative was devoted to explicating concepts of privacy and information security. The report asserts that privacy is about

the individual and about relationships between the individual and the institution. Two types of privacy were identified, each of which must be addressed in university values, principles, and policy:

- *Autonomy privacy*: an individual's ability to conduct activities without concern of or actual observation; it is related to concepts such as the First Amendment's freedom of association, anonymity, and the monitoring of behavior.
- *Information privacy*: the appropriate protection, use, and dissemination of information about individuals. It is about an individual's interest in controlling or significantly influencing the handling of information about himself or herself, whether it is an academic, medical, financial, or other record.

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

Figure 1 depicts the domains covered by autonomy privacy, information privacy, and information security, and the overlaps between them.

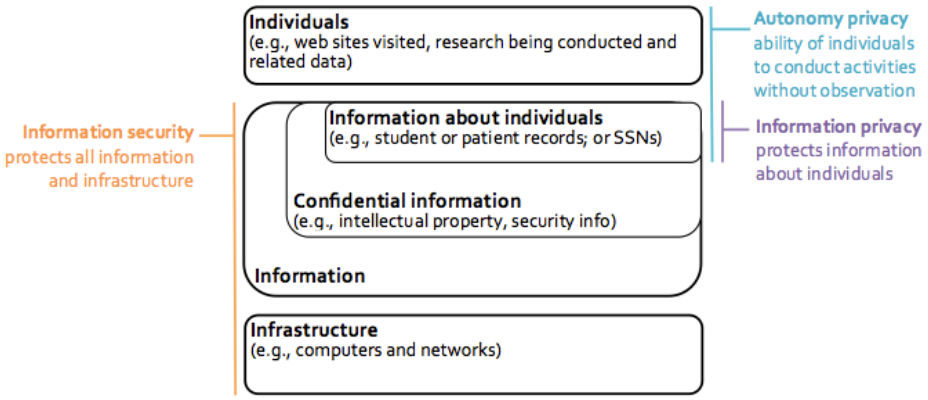

Figure 1: Relationships between autonomy privacy, information privacy, and information security.

Privacy Values

Rather than drafting policy for today's environment, the Steering Committee established a values statement that is expected to stand the test of time. This proactive approach allows consistent policies to be developed and adopted in response to changing technologies, institutional contexts, and social norms.

The values statement asserts that the University of California respects the privacy of individuals. Privacy plays an important role in human dignity and is necessary for an ethical and respectful workplace. The university must balance its respect for autonomy and information privacy with its other values and with legal, policy, and administrative obligations.

Thus, the university continually strives for an appropriate balance between the following:

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

Privacy Principles

Similarly, the Initiative established privacy principles derived from the UC Statement of Privacy Values. These, in turn, build upon accepted privacy principles such as the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (The Organisation for Economic Co-operation and Development, 2013) and the Federal Trade Commission's (FTC) Fair Information Privacy Practice Principles (Gellman, 2014). The UC Privacy Principles are intended to guide policies and practice in conjunction with information security objectives of protecting the confidentiality, integrity, and availability of information resources.

Members of the university community are expected to uphold autonomy privacy, as defined above. The university is also committed to providing individuals with a reasonable degree of control over the collection, use, and disclosure of information about themselves, which is information privacy. Among the principles that guide information privacy policies and practices are privacy by design; transparency and notice; choice; information review and correction; information protection; and accountability.

Privacy Balancing Process

Recognizing that the interests of the institution and the individual are sometimes aligned and sometimes not, and that different types of privacy are sometimes aligned and sometimes not, the report establishes criteria for balancing these factors in each situation.

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

The balancing process must expressly consider the parties' interests, benefits, burdens, and consequences associated with the proposed action. Each analysis will differ depending upon the action and the interests involved. A party in such an analysis may be, or represent, an individual, a community, or the university, recognizing that parties may overlap or that a party may have multiple roles. Among the factors to be considered in privacy analysis are these:

- What are the benefits to each party in successfully asserting privacy interests or a specific policy stance? What are the burdens, impacts, and risk to each party if the proposed action is not taken?
- What alternative approaches, or reasonable privacy protections, might be used in conjunction with the proposed action to make it less intrusive?
- What are the costs, whether in money, time, effectiveness, or other metrics?
- What actions have been taken (or could be taken) by each party to protect their own interests?
- What new technologies or processes might mitigate the privacy concerns, now or in the foreseeable future?

Recommendations

The Privacy and Information Security Steering Committee Final Report made four recommendations. While these are stated in the context of UC governance, they are readily adaptable to other institutional environments:

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

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

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

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

Recommendations 1, 2, and 4 were accepted in full, whereas recommendation 3 was deferred for future consideration (Lucas et al., 2013). However, the privacy officials of the 10 campuses already have begun to meet on a regular basis.

Conclusions

The final report of the UC-wide initiative is now being disseminated widely and its recommendations are being implemented across the entire University of California system. In some cases, duties of existing staff are being expanded to include these responsibilities; in other cases, new staff were hired. Similarly, the duties of some existing boards were expanded and

new boards were formed. At UCLA, which has had an active Privacy and Data Protection Board since 2005, implementing this framework has led to increased awareness of privacy issues on campus, a deepened understanding of governance, and expanded operational and strategic roles for the Chief Privacy Officer and the Governance boards. The principles have proved useful to address a wide array of privacy-related issues such as diversity and institutional climate, surveillance, online education and educational analytics, distinctions between public and private uses of information about faculty and students, the formation of public-private partnerships, and governance of data about faculty, students, and staff. During two years of meetings and consultation across the UC system, we found that few universities have taken such a holistic approach to privacy and information security. Faculty, administrative, and student concerns were addressed in the UC process to develop an integrated model of values, principles, and governance that balances privacy and information security interests. The report deliberately avoids mention of specific technologies, recognizing that policy, principles, and values must transcend today's technical infrastructures. Rather, we developed a framework that is expected to serve the university well into the future. We offer this holistic framework as a model for other universities and institutions of higher education.

References

Academic Freedom. (2014). *American Association of University Professors*. Retrieved April 29, 2014, from http://www.aaup.org/issues/academic-freedom

Gellman, R. (2014). Fair Information Practices: A Basic History. Retrieved from http://www.bobgellman.com/rg-docs/rg-FIPShistory.pdf

Lucas, G., Vacca, S., & Yudof, M. (2013, July 2). Transmittal Letter and Response to UC Privacy and Information Security Report. University of California, Office of the President. Retrieved from http://ucop.edu/privacy-initiative/yudof-response.pdf

Privacy and Information Security Initiative, Final Report. (2014). *University of California, Office of the President*. Retrieved May 8, 2014, from http://ucop.edu/privacy-initiative/

The Organisation for Economic Co-operation and Development. (2013). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Retrieved July 31, 2014, from http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm