UCLA Board on Privacy and Data Protection

Meeting Summary
Friday, December 12, 2014 | 10:00 AM-12:00 PM | 5628 Math Sciences (IDRE Portal)

Attendees:
Burton Swanson (phone), Amy Blum, Andrew Metz, Christine Borgman, Ed Pierce, Frank Wada, Julian Pellico, Kent Wada, Leah Lievrouw, Lubbe Levin (phone), Marti Arvin, Ross Bollens; Kelly Arruda (resource)

Guests:
Dr. Andrew Treloar, Director of Technology, Australian National Data Service
Adrienne Dellinger, PhD student, Graduate School of Education and Information Studies

A. Welcome (Burt Swanson)

1. Approval of minutes
2. Introduction of guests

B. Big Data and the UCLA Data Governance Task Force (Christine Borgman, Kent Wada)

Two scenarios catalyzed the taskforce: (1) the growing scope of data about members of our community and (2) the rising number of nuanced areas needing guidance.

Charge

The University is continually generating a tremendous amount of data. Within this mass of data, there are opportunities to promote operational efficiencies, augment instructional experiences, and support governmental reporting requirements. At the same time, we know that outside organizations are interested in commercial use of our data. And there is concern about inappropriate use of data, whether deliberate or unintentional.

Solid data governance works to ensure trust and establishes a consistent process for addressing campuswide data issues, while established principles can guide use of data. EVC and Provost Waugh charged a joint Senate-Administration work group with establishing principles, as well as a governance structure to address ongoing complex data issues.

1. **Principles:**
   Principles serve as a guide and set consistent "expectations about ethical and appropriate use of data, as well as security, accuracy, and compliance obligations."[1]
2. **Governance structure and operations:**
   Establishing a structure and process ensures expectations are met and that data issues can be addressed consistently/strategically across campus, including mechanisms to address new data requests, resolve conflicts, and align policy and practice among data stewards.

Areas of concern for two major data sets

1. Faculty data:
   a. Productivity and metrics
   b. Ethics in polices (Opus, etc.)
   c. Elsevier, Thomson Reuters, McMillian mine citations, etc., and they are competitive in seeking partnerships with universities. They want access to our data, so that they can tell us about us; how can we leverage our own data?

[1] Charge letter: https://ccle.ucla.edu/pluginfile.php/708990/mod_resource/content/0/Charge Letter.pdf

2. Student data:
    a. Incredibly detailed data capture – from how much time is spent on a particular problem to logging keystroke data; how do we appropriately utilize this data?
    b. Just because we can easily capture more and more data does not mean that we should; we need to continually ask ourselves whether a particular data capture and use is appropriate. Traditional data governance focuses on being a good steward of data. The work of the group goes beyond this to the nuanced work of *big* data governance – it requires taking an ethical look at the "should we?" questions and perform a risk evaluation whereby we weigh the costs/risks/benefits and then determine whether it matches up to our values.

Currently, when there are privacy implications, where does one go? You may start by going to the IRB. However, it may fall outside the purview of the IRB but still have privacy and ethical components of concern. Where does one go, and secondly, what guidance do we use to deliberate and confirm the activity is alignment with our values?

Can we leverage an existing (or subset of an existing) governance group to take on these issues, or do we need to create a separate entity? We don't want to re-invent what has already been accomplished. Rather, we want to build on existing structure and leverage existing guidelines, principles, etc., and determine where we want to break new ground.

Feedback/Discussion from Board

We need clarification on how this could intersect with the Board and a strong articulation of why and how it would go here. With so many dimensions of data to consider, would it be possible to set up a one-stop shop?

There are a lot of faculty members that are enthusiastic about using tools, some of which are open source, no cost, no contract, and not vetted by university officials.

While there is enthusiasm for moving forward in this area, there is also concern about the level of understanding of data capture. We may not be mature enough to have standards yet, as many individuals do not understand the ecosystem. It is still invisible to most. There is a transparency issue here.

For some areas not governed by law (e.g. third party MOOCS are not subject to FERPA), we can mitigate via contracts; even if FERPA does not apply, we can set our own standards via contract. Of course, Purchasing and Contracts and Grants need to be represented in these discussions (Appendix DS – approved language for developing contracts).

C. Raising Awareness of privacy obligations and expectations within the UCLA community (Amy Blum, Lubbe Levin, Kent Wada)

C-1: General awareness document

This is an attempt to set expectations for new employees, especially for those coming in from the private sector, about what academic freedom is and how it drives a lot of our policies. And it introduces the concept of the balancing process by which information may or may not be held for exemption in public records requests. The first document (C-1) is a sort of preamble – a value statement applicable across our community of faculty, staff, and students.

Public Record Act requests have gone up in the last 2-3 years. The campus now has a reference for dealing with requests regarding scholarly communications. They employ a balancing process where they are able to weigh disclosure against the value of not disclosing particular information. If anything in the content is subject to redaction, it gets held from disclosure. For example, a dialogue between colleagues that includes both personal and professional discussion may have a portion of the content redacted. We engage in dialogue and a process for determining whether content is scholarly communication or the administrative work of the University. Under FERPA, there is more power to withhold; with subpoenas, we have less power to withhold. Also, remember the University data on your personal device is still University data. We need to keep in mind that the public has an interest in seeing the business of the University.

Suggestions

There is a suggestion to add scholarly communications documents to the packet. Appendix A begins the awareness process, but it may need to be more explicit.

1. Add a note about third parties and what they have access to (e.g., what does Google have access to and what are they tracking?).
2. Create a separate section for contractors.
3. The first document (C-1) is very abstract, where the department document (C-2) is much more concrete. Perhaps add some of the language from the first document into the concrete document and incorporate the rest into the UCLA Statement on Privacy and Data Protection.

C-2: Informing new employees of campus policies and practices with respect to data and devices

This document has been developed as a customizable checklist for departments. It is meant to help set expectations in a concrete manner and establish consistency across campus, while also allowing room for customization. The document educates individuals so that they can make informed choices about their use of technology and their handling of communications, and it puts the onus on the individual to clean their personal documents before separating from the University. It acknowledges academic freedom right at the beginning of employment, which may not even be a consideration in some areas today.

Feedback/Discussion from Board

1. On-boarding:
    a. Perhaps some of the abstract language can be merged into to this document as well.
    b. Suggest that employees segregate business and personal (e.g., Capital Records functions on share drives for business).
    c. It may be helpful to include concrete examples/guides of what is considered personal vs. University business, with the understanding that sometimes it's a judgment call. One may think it is personal, but it could be disclosed in litigation; education can help individuals make informed choices about their use of technology.
    d. There are a number of statements that caution the overlap of work and personal correspondence, but the document does not include an established definition.
    e. The term "restricted" in used in the two documents. If this is a policy statement, please clarify.
    f. What is the threshold for nonconsensual access? We make a reasonable effort to determine the need to access and to contact the individual. For example, if a faculty member leaves and his/her old boss wants to know why, that supervisor may try to go through a nonconsensual process to access, but he/she may not get approved. It may not be considered appropriate or reasonable access.
    g. Create a consistent off-boarding/exit document.
2. Other:
    a. Our retention policies set schedules for documents, not email. Perhaps this needs to be addressed.
    b. Work can often involve individuals from outside the University; people may be cc'd on emails that may be accessed. Those emails may also be subject to access according to other states' laws. Perhaps include a note about this in the document.
    c. We could consider developing separate categories of individuals and treat their documents and/or communications accordingly.

C-3: Proposal for a campuswide approach to the disposition of electronic communications records of separated staff and faculty

Within the last few years, the UC Office of the General Council (OGC) has looked at policy and developed a rationale that states when an employee separates from the University, he/she is no longer a "holder" of records, and the University does not need consent to access his/her electronic records.

Though we are currently allowed to access electronic communications after individuals separate from the University, our current practices are not consistent. The suggestion is to get our policies and practices in alignment with the OCG rationale for separated staff and faculty (excluding Emeriti, Senate faculty, etc.) by solidifying the interpretation in policy and building protections around it as necessary. This would consist of a two-step approach:

1. Determine a campuswide approach;
2. Then take that approach and make it operational policy.

Concerns

This proposal does not seem to respect the privacy of separated faculty. From the viewpoint of an academic, a faculty member has correspondence with colleagues that should remain as private communications even after leaving the University.

We need to do a much better job of raising awareness and setting expectations. We are starting this discussion with the Board because we understand that are lots of legitimate perspectives to balance.

D. Data Privacy Month Activities (Kelly Arruda)

There are a few events scheduled during Data Privacy Month (January-February 2015). The Hammer Museum will be screening *CitzenFour*, the Laura Poitras documentary about the Edward Snowden NSA revelations. The museum will also be hosting discussions with privacy advocates, James Bamford and Julia Angwin. Chris Borgman suggests we may be able to invite James Bamford to visit the campus during his stay. Kelly will work with Chris and the Office of the Campus Chief Privacy Officer on the logistics of making this happen as part of the Board's tenth anniversary celebration.

In February, the Office of the Campus Chief Privacy Officer, the Office of Information Technology, and Insurance and Risk Management are hosting a Data Protection Seminar with numerous mini presentations on pertinent data protection subjects.

Also in February, the Library and the Office of the Chief Privacy Officer will be co-hosting a presentation by Aljazeera journalist, Michael Keller, and graphic novelist, Josh Neufeld, on their recent privacy collaboration, Terms of Service.