UCLA Board on Privacy on Data Protection

Thursday, October 8, 2015 | 3:00-5:00 PM | 5919 Math Sciences

Attendees:
Dana Cuff (Chair), Burton Swanson, Amy Blum, Andrew Wissmiller, Charles Taylor, Christine Borgman, Edwin Pierce, Frank Wada, Kent Wada, Marcia Smith, Marti Arvin, Maryann Gray, Mike Story, Neil Wenger; Kelly Arruda (resource)

Guests:
Alyssa Shauer, Student, School of Law; Irene Pasquetto, Student, GSEIS; Jennifer Pierre, Student, GSEIS

A. Welcome & Introductions

B. Overview of Privacy and Data Protection at UCLA 2015-16

Dana Cuff, Jim Davis, Kent Wada

Action: Information and Discussion

With the constant growth of big data, we are continually looking at ways to protect data and infrastructure. Progress is being made in considering privacy in planning efforts across the system. The UC Privacy and Information Security Initiative’s (PISI) work has influenced this area, and privacy boards have been established at each campus. Across higher ed, privacy boards (where they exist) are mainly operational. The Board’s deep review of privacy concepts over the years has strengthened its ability to address operational privacy and data governance issues in a thoughtful and constructive manner.

Given the evolving technology landscape and the UCLA cyber attack event earlier this year, the Board is uniquely poised to share its expertise and insight in forthcoming efforts. The Board needs to decide how to actively participate and focus efforts.

Potential areas for input or focus:

1. Take the upcoming mandatory cyber training. Then assess the training and provide feedback. Perhaps we can provide a thoughtful, constructive critique (as we did for the climate survey), suggest a more sophisticated approach to teaching cyber security, measure outcomes, etc.

2. Work with applicable groups that have influence over privacy and data protection efforts (Cyber-Risk Center of Excellence, the UCLA Coordinating Committee on Information Security and Privacy, etc.)

3. Use an hour of our meetings to flesh out a topic, so that over the course of the year we can develop a useful set of insights and/or scenarios to help inform discussions and decisions across the system.

4. Sponsor a graduate student study (similar to the Anderson MBA project on file sharing – p.5-6).

Action Items:

1. Coordinate with the EVC’s office to schedule a briefing of current and upcoming cyber efforts and activities.

2. Compile a list of questions to put forth to the Cyber Security Center of Excellence, such as:
   - Can we send a delegate?
   - How can we provide input as to the experts that get designated to the center?
   - What metrics are being employed?

3. How can we collaborate with the new UCLA Coordinating Committee on Information Security and Privacy?
C. Security Program
Andrew Wissmiller, Kent Wada
Action: Information and Discussion

D. New UCLA Coordinating Committee on Information Security and Privacy
Jim Davis, Andrew Wissmiller
Action: Information and Discussion

(Summaries of agenda items C. and D. have been combined below.)

The University is a data rich environment that presents certain kinds of risks. While the institution promotes openness and access, it also has to provide a secure environment from malicious intrusions. The evolution of individual hackers to criminal groups and even nation-state attacks requires that the model for addressing cyber security also evolve.

The 5-Point Plan
Given the cyber attack earlier this year, in which an investigation is still underway, UC President Napolitano has put forth a 5-point plan with 120 days progress timeline. The plan includes:

1. Inventory and access current cyber environment and vulnerabilities
2. Develop plan and governance approach to reduce risks
3. Participate in systemwide efforts
4. Schedule regular discussions with executive level campus officials to review campus cyber risk management
5. Ensure adequate staffing and budget to enhance initiatives

The campus has submitted a plan to UCOP, and campus officials will be sharing additional information shortly.

The assessment plan will call for an inventory and risk assessment of all data, and profiles are being developed as standards in protecting data. As plans develop, they will be put forward to the various governance groups for review and input, so we can collectively move the campus forward in strengthening privacy, data protection, and data stewardship.

Training Requirement
There will also be mandatory UC cyber security training released shortly. The modules follow the NIST framework. While the training provides a good foundation, gaps remain (e.g., the training does not currently offer a Spanish version of the modules). The Board could consider ways of enhancing this learning opportunity:

2. Are there studies that support this type of training as useful?
3. How do you know whether learning is happening?
4. What is the best way to teach students about cyber security?
5. What are other institutions doing in this area?

This is an opportunity to look at what it means to be a digital citizen today. It is not enough to move seamlessly between devices; digital citizenship encompasses a holistic approach and board understanding of the technology and data landscape. It also provides an opportunity to move away from the concept of data ownership and toward highlighting and embracing data stewardship.
**UCLA Coordinating Committee on Information Security and Privacy**

In addition to the 5-point plan, the campus is required to make a more distinct connection between the campus side and the medical system. Traditionally, the two have remained fairly separate as the two sides have separate focuses; the medical system has a strong focus in information privacy of HIPAA data, while the campus has a strong investment in autonomy privacy. The two sides will continue to focus on their respective areas but will actively collaborate and leverage each other’s expertise where possible. Various governance boards on campus have been staffed to ensure a cross between campus and medical system representation.

**Cyber Risk Governance Committee**

At the UC level, a Cyber Risk Governance Committee has been established with a designated representative from each campus that has a broad perspective of the campus; UCLA’s designate is Executive Vice Chancellor and Provost Scott Waugh.

**E. Landscape Topics 2015-16**

Dana Cuff, Kent Wada

*Action: Information and Discussion*

**Data Classification, Data Governance and Stewardship**

An assessment across the system found 35 data class systems. Some time back, UCLA leveraged work done by UC Berkeley to draft a UCLA campus data classification standard. Meanwhile a UC group is currently working on a systemwide data classification standard, so the UCLA version is currently on hold.

While the end results of the system version may be a bit different than what the campus started with, similar processes are being employed. The data classification standard uses a risk-based approach to access the institutional impact of a data compromise and sets data protection profiles accordingly. At the same time, the standard will set minimum standards for protecting data across campus.

There is concern of locking down systems too tight. However, even if an individual does not have sensitive data, the nature of having an open environment may allow access to enter other areas that do have sensitive data. Balancing risk and public access will be a difficult ongoing process.

Additional areas to be considered: scope, ownership vs. stewardship, data governance, risks, regulatory requirements, use cases, and embedding balancing process into the data classification standard.

The Data Governance Task Force has been working through the summer and will be sharing insights with the Board soon.