

Collaborative Tools Strategy

University of California, Berkeley

Spotlight: Legal and Policy

Goal 1 of the Campus Collaborative Tools Strategy for UC Berkeley is to "Provide enhanced information and guidance to all members of the campus community on collaborative tool selection and use." Goal 1b further specifies, "Provide guidance around storing and using university data in collaborative tools."

Among the recommendations related to this goal are that the campus clarify, rationalize, and publicize the risks associated with storing and using campus and University data in collaborative tools. The purpose of doing so is to help provide clear guidance to the campus community about what types of data can be stored in, and what types of collaborative activities can be performed within, various collaborative tools and services, in a manner that protects restricted and sensitive data, and reflects the campus's legal, policy, and contractual concerns. This Spotlight document provides more in-depth discussion regarding those recommendations

Storing university data with services that are not under the campus's control has long been occurring. Some obvious examples include university-related email messages and attachments that are often routinely forwarded or mailed to personal accounts on services such as Gmail, Hotmail, and Yahoo! Mail; university-related photos that are published on photo sharing and web-accessible file storage sites such as Photobucket and Flickr; and videos of lectures from selected campus courses and major university events that are made available to the public via iTunes and YouTube.

This practice is expected to become more widespread — and often will be campus-sanctioned — when collaborative tools and other IT services are sourced from outside the campus, particularly via the software-as-a-service (SaaS) model.

However, doing so introduces important legal, policy, privacy, and contractual issues. Some of the most prominent issues relate to protecting restricted and sensitive data; to concerns about the discovery of data stored with outside providers within the context of national security, criminal, or civil matters; and to protecting university data and campus customers when an outside provider ceases to provide a service or precipitously changes its service offerings, terms or pricing. Some major areas into which these issues can be categorized include:

1. Restricted and sensitive data handling.

This area covers how UC Berkeley campus data that is restricted by law or policy – for instance, health data subject to the Health Insurance Portability and Accountability Act (HIPAA), and student data subject to the Family Education Rights and Privacy Act (FERPA) – can be stored and managed appropriately on services provided off campus, or alternately, be kept from being stored on off-campus services.

General guidelines for handling certain types of restricted or sensitive data, currently focused on how such data can be protected when stored on campus servers and workstations, are provided through the campus's Minimum Security Standards for Electronic Information, adopted in September 2008 (<https://security.berkeley.edu/MinStds/elecinfo.html>).

2. Legal issues.

This area deals with how subpoenas and other types of requests for discovery of data, in national security-related, criminal and civil processes, are handled when university data is stored with outside providers. In particular, there is a high level of sensitivity at UC Berkeley to the possibility that recent laws¹ may permit US Federal agencies to request data from service providers without the Berkeley campus or the University of California being informed. There is also a concern that service providers might in some cases be the only parties with legal standing to respond to discovery requests, rather than the University, and that they may not contest these requests as vigorously as the University might. Either of these circumstances could have immensely deleterious effects on the campus's and University's culture of providing a haven for intellectual freedom.

In addition to deeply-held concerns in that area, a number of campus data stewards and IT providers have expressed misgivings around the legal implications of storing other types of particularly sensitive data with outside providers. For instance, there have been concerns expressed about whether storing data with off-campus providers may impact the process of legal discovery related to faculty hiring and tenure decisions and other similarly high profile matters that occur during routine university business. Protection of intellectual property, particularly speculative early work that may ultimately lead to the production of commercially valuable products, processes or services, is another area of expressed concern when storing data off-campus.

3. Policy issues.

This area relates to how campus and university policies, such as UC Berkeley's Campus Online Activities Policy and Computer Use Policy, and the University of California's Electronic Communications Policy, can be enforced within the context of an outside provider's facilities. This issue includes the need to resolve issues related to how detection of violations, notification to affected parties and access to relevant data can be handled between the campus and the service provider.

4. Contractual issues.

This area is concerned with how contracts with outside providers can be entered into in a timely manner, resolving any differences between the providers' terms and the University's interests to both parties' satisfaction. This issue may require that the University examine practices that have led to extended contract negotiations, which may become increasingly ill-matched to the pace of technological innovation in the collaborative services arena and the number of providers offering services of interest to the University. For instance, the University often requires outside providers to remove contract clauses indemnifying them from harm. However, outside parties that are providing services free of direct charges to the University may be reluctant to accept such modifications.

One notable concern, with both contractual and technical components, is how university data stored with outside providers can be protected from loss or damage if a provider goes out of business, is acquired, changes its business model, materially changes its terms of service, or has a security breach or operational failure. For example, if the only copies of high resolution images taken of items found during an anthropological dig were stored with an outside provider, there might be concerns that service could decide to recompress those images to reduce their size, also reducing their resolution and introducing distortions; or might lose them altogether.

These issues will need to be closely examined over time, and resolved to the greatest extent possible, in order to:

1. In 2001, the USA PATRIOT Act greatly expanded the permitted uses of National Security Letters (NSLs) by Federal agencies, such as the Federal Bureau of Investigation. NSLs do not require judicial approval, and they also contain a gag order that prevents recipients from even discussing them with anyone. Subsequent reauthorizations of that Act carried forward these broad permissions related to the issuance of NSLs, and added penalties for violating their gag orders.

- Work toward removing barriers to entering into mutually beneficial partnerships with outside providers;
- Provide guidance to IT providers and data custodians on how to appropriately manage university data when working with outside providers; and
- Identify under what circumstances it may be inappropriate to store university data outside strict campus custody.

These issues may be difficult to resolve to the full satisfaction of the many stakeholders involved. Yet agreements and approaches that safeguard the campus's data and protect the University from liability, while still allowing its members to use services from outside providers, are essential to the notion of "embracing the chaos" that is at the core of this strategy. Even if the campus does not contract with outside providers to provide enterprise-scale collaboration tools to the campus community, both formal and informal uses of those providers' services are already occurring today and are only likely to increase over time, as is the quantity and variety of university data stored outside the boundaries of the campus. At the very least, clear and helpful guidance must be provided to campus users.

In this area, the early experiences of other higher education institutions will likely prove very valuable, as will any direct experiences that the campus can gain by rolling out pilot services – or other services of limited scope – that store campus data with outside providers.

Finally, since both law and UC policy is subject to change, as are the business practices of outside providers, any formal or working agreements in this area will also need to be re-examined on a periodic basis.