# Effective Acquisition and Appropriate Use of Internet-based Services and Software:

# Vendor Terms and Conditions

Workgroup Report for ITLC
August 9, 2013

Janine Roeth (SC), Chair
William Allison (B)
Stephen Benedict (OP)
Jon Good (OP)
Lisa Ho (B)
Stephen Lau (OP)
Patrick McGrath (B)
Kevin Schmidt (SB)
Isaac Straley (I)
Thomas Trappler (LA)
Cynthia Vroom (OGC)
Kent Wada (LA)
Cheryl Washington (D)
David Willson (B)
Gabriel Youtsey (D)

## Executive Summary

Internet-based services and software (often free or low-cost) are widely employed by University departments and employees. These services and software have become part of our everyday lives and their widespread use – likely in the tens of thousands when aggregated across the UC system – is further spurred by the ease of acquisition: the acceptance of terms of use by an individual simply clicking on an "I agree" button (aka "click-through").

By clicking "I agree," it is all too easy for faculty and staff to unknowingly accept terms that create risk both to the individual and to the University. Bypassing the University's procurement process skips controls to evaluate and mitigate risk, ensure appropriate contract terms, and assure compliance with pertinent UC policies and practices. At the same time, the procurement process does not distinguish well between high-risk and low-risk circumstances in this area and can inappropriately and significantly burden low-risk use with the "gold standard" process of high-risk situations.

A cross-functional, multi-campus workgroup was convened to identify where the use of these services and software under vendors' standard terms and conditions create risk, either through conflict with University policy or by otherwise disadvantaging the University. The group's analysis identified five major areas needing further work to appropriately realign University policy and practice with the reality of Internet-based services and software: indemnification, risks and impact, favorability, acceptance of terms, and conflicts or ambiguities with the UC Electronic Communications Policy.

For each area, the workgroup offers recommendations for next steps (see the table on the next page). While functional offices are identified that are best suited to take lead, the workgroup believes that cross-functional involvement is imperative as these issues are complex and intertwining. As such, this report illuminates a path forward, but one that will require strong, coordinated executive support from several areas in order to proceed.

| FINDING | RECOMMENDED ACTION | NEXT STEPS TO BE TAKEN BY |
|---|---|---|
| **Indemnification**<br>The standard language in most click-through terms conflicts with a Regents Standing Order. | • Review current interpretations of Regents Standing Order 100.4(dd).9 and consider updating relative to new developments such as cloud computing.<br>• Develop a proposal for the Regents that delegates authority for providing exceptions to the Regents Standing Order to some entity that may be better positioned to evaluate risk in the University's operational context. | • Office of General Counsel or Ethics, Compliance and Audit Services |
| **Risks and Impact**<br>Click-through terms are generally not expansive enough to handle risks associated with *sensitive data types* or *use in critical business functions.* Users must be aware of these risks. | • Provide education and self-service evaluation tools to end users to enhance ability to determine appropriateness of services relative to data and business function risks.<br>• Identify and provide consultative resources to support more complex end user decision-making processes. | • Information Technology via ITLC |
| **Favorability**<br>Clicking-through precludes negotiation of terms between the University and the vendor. Click-through terms tend to include compromises in favorability, including general, economic, and academic freedom. | • Engage the relevant business partners in the review of impacts of click-through services on standard business practices or policies to be consistent and inclusive of operational requirements.<br>• Remove barriers to easy adoption of public sector negotiated agreements, e.g., NET+, CENIC, federal/state.<br>• Develop a robust information sharing mechanism for vendor assessments. | • Risk Services, Office of General Counsel, Procurement Services / Business Contracts<br>• Procurement Services, Information Technology via ITLC<br>• Information Technology via ITLC |
| **Acceptance of Terms**<br>Most individuals accepting click-through terms do not have the authority to bind the University to terms. This is compounded by the merging of personal and institutional devices and data. | • Extend existing models for low cost procurement delegations to allow low-risk technology purchases to go through quickly using click-through terms.<br>• Develop guidance on when a click-through is being done on behalf of an individual and when it is being done on behalf of the University. | • Procurement Services |
| **ECP Conflicts or Ambiguities**<br>Click-through terms include areas of potential conflict or ambiguity with the UC Electronic Communications Policy, especially as related to consent and access to data. | • Update UC privacy policies[1] to address discrepancies between vendor and campus standards for privacy, including consent and vendor access, definition of content and individual responsibilities. | • Privacy, Senior Vice President/Chief Compliance Officer and Vice President of Information Technology Services /Chief Information Officer [2] |

[1] Consistent with the President's Privacy and Information Security Initiative. Final initiative report of the Steering Committee available upon request. A summary can be found in the background materials used to present this initiative to the UC Regents.

[2] Senior Vice President and Chief Compliance and Audit Officer Sheryl Vacca is the executive point for the Privacy and Information Security Initiative.

# Problem Statement

Internet-based services are employed by University departments and employees to broad institutional benefit: for example, cloud storage and computation (Dropbox, Amazon Web Services), social media (Facebook, YouTube, Wordpress), videoconferencing services (Skype), calendaring (Doodle) and surveying (SurveyMonkey). Similarly, free and low-cost software – such as the Firefox browser, Adobe Flash plugin, Adobe (PDF) Reader, and Linux operating system; as well as a multitude of apps for mobile devices – are routinely deployed on University equipment. These services and software have become part of our everyday lives; it is likely there are tens of thousands of uses when aggregated across the UC system.

Internet-based services and software with a cost may be acquired by providing a credit card and accepting terms of use via an "I agree" button ("click-through"). The ease of this process can belie the need to follow UC procurement processes ensuring appropriate contract terms and conditions and compliance with pertinent UC policies (BFB-BUS-43, Materiel Management). When procurement does follow standard processes, resulting negotiations can be time-consuming, with vendors often unwilling to participate.

With click-through services and software, the appropriate process for review and acquisition is unclear and UC faculty and staff are able to access and use the products by merely accepting the click-through agreements. UC faculty and staff may be agreeing to terms and conditions without knowledge or consideration of the potential risks to themselves or to the University.

The terms and conditions of these click-through agreements are often in conflict with University policies in areas such as liability, privacy and security. Yet there are neither controls nor user guidance in identifying risk factors and acceptable risk that informs decision-making and enables the University to take advantage of software and Internet-based services without always going through the time-intensive "gold standard" procurement processes.

# Approach

A cross-functional, multi-campus workgroup examined the click-through terms and conditions ("click-through terms") of commonly used services and software ("Candidate Vendors"), identifying where the terms were not in alignment with University policy or otherwise presented a disadvantage.

The Candidate Vendors were:

- *Dropbox,* popular and pervasive, and an example of storage and collaboration tool used by both individuals and units/campuses.
- *Apple iCloud,* a major vendor and example of cloud storage for applications
- *Facebook,* popular and pervasive and an example of social media.
- *YouTube,* a consumer app separate from contracted Google Apps for Education and an example of a digital media app that may be used in instruction or for institutional purposes.
- *Google Analytics,* a major vendor and an example of institutionally-used web analytics.
- *Evernote,* an example of a productivity tool with a variety of platforms and storage locations.

The workgroup analyzed areas of the terms and conditions derived from checklists developed by cloud computing contract experts.[3]

- Acceptable Use Policy
- Clarify Rights and License (University and End User Data)
- Credit Card Information
- Data Access/Retention/Transfer
- Data Location/Residency/Export Controls
- Fees
- FERPA Designation
- Governing Law
- Health Information
- Indemnification
- Information Security and Integrity
- Insurance
- Limitation of Liability
- Privacy
- Representations and Warranties
- Response to Legal Orders/Demands for Data
- Supplier Outsourcing/Subcontractors
- Vendor Modification (Terms or Service)

[3] Stephen Benedict (OP) and Thomas Trappler (LA) had each compiled cloud computing checklists informed by their procurement experience and other sources (e.g. Educause, NIST, Cloud Security Alliance).

# Findings and Actions

## 1. INDEMNIFICATION

Regents Standing Order 100.4 (dd).9 requires specific authorization from the UC Board of Regents to enter into agreements where the University assumes liability (e.g., provides indemnity) for the acts of parties beyond the University's control. The University cannot provide indemnity for the acts of third parties without this authorization. This requirement applies to agreements, including vendor agreements and is common in public entities, such as UC.

Many vendor terms and conditions include an indemnification clause that is in conflict with this standard; yet it is impractical to obtain approval from the Regents before entering into each of them at this scale. Where there is an opportunity to negotiate terms and conditions, most often the University is able to negotiate language that is acceptable to all parties. With free and low cost services, most vendors are uninterested in negotiating changes to their terms and conditions.

From the workgroup's analysis, it becomes clear that the risk of using the Internet-based software and services under consideration can range from low to potentially very high (see the next section, Risks and Impact). There needs to be a vehicle by which this risk can be evaluated so that the level of attention and effort put forth by the University is commensurate with risk.

### Recommended Action

- Involve Office of General Counsel (OGC) to review current interpretations of Regents Standing Order 100.4(dd).9 and consider updating relative to new developments such as cloud computing.
- Engage representatives from OGC, Risk Services, and Procurement Services to develop a proposal for the Regents that delegates authority for providing exceptions to the Regents Standing Order to some entity that may be better positioned to evaluate risk in the University's operational context.
- Leverage agreements that have been negotiated by other groups, (e.g., Internet2, GSA, CENIC, CSU) that already address indemnification.

## 2. RISKS AND IMPACT

Use of "click-through" services and software is widespread – as noted earlier, likely in the tens of thousands when aggregated across the UC system – and tightly integrated into devices and functions of everyday life. However, use of such services and software can represent risk ranging from low risk to potentially very high risk.

The level of risk is primarily dependent upon:

- The sensitivity of data being stored or processed in the cloud; and
- The business criticality of the function being moved to the cloud (functions essential to campus operations requiring high availability).

Services and software that store content in the cloud represent high risk when sensitive data is involved, due to the potential for unauthorized access (including that released through collaboration, where someone other than the data owner controls access). Standard vendor click-through terms do not effectively address risk associated with placing sensitive data or business critical functions in the cloud. End users often do not have sufficient awareness of these issues to effectively address them in the solution selection process and have few tools to help them do so. See the Supplement for more information on risks and impacts in these areas.

On the other hand, many common services and software generally represent low risk: e.g., the popular open source Firefox browser or the Doodle service for polling meeting times. It is important to have a way to avoid unnecessarily burdening these low risk circumstances. This first requires being able to distinguish such circumstances: e.g., whether content is involved and of what type, or whether use is collaborative or analytical.

### Recommended Action

- Provide education and self-service evaluation tools to end users to enhance ability to determine appropriateness of services relative to data and business function risks.[4] See examples from Princeton, University of Michigan, University of North Carolina, University of Wisconsin–Milwaukee, and UC Berkeley.
- Identify and provide consultative resources to support more complex end user decision-making processes (e.g., IT vendor management, policy, security, technical, legal, procurement, risk management).

[4] Enterprise Risk Management is working on tools that help with general risk assessment and appetite that would be useful to track and leverage. Also, multiple campuses have advice for users on free/low-cost services, though it is not aligned systemwide. Some campuses are also working on a Data Classification Standard (for example, the Berkeley model linked above) that will help inform risk assessments, though again these are not aligned systemwide at present.

## 3. FAVORABILITY

Click-through precludes negotiation of terms between the University and the vendor. Click-through terms tend to include compromises in favorability, including general, economic, and academic freedom, that may otherwise be addressed in the procurement process.

- Terms that affect favorability include the areas of: *Governing Law*, *Limitation of Liability*, *Representations and Warranties*, *Response to Legal Orders*, *Data Access/Retention/Transfer*, *Vendor Modification (Terms or Service)*, *Third-party Audits*, *Service Level Agreements.*
- Terms that have an economic effect include: *Fees*, *Insurance*, *Vendor Modification (Terms or Service)*, *Service Level Agreements.*
- Terms that potentially affect academic freedom include: *Acceptable Use Policies.*

Many of these areas are guided by best practices or in some cases by policies that have not yet incorporated the impact of click-through services. Current practices that depend upon access to University records may encounter hurdles when stored on non-University services without negotiated terms. Individuals are also responsible for understanding that the University should have access to University records, and knowledge of the location of University records, even when those records are maintained on non-University managed systems and services. There is a need to revisit these practices/policies in a more comprehensive manner – to avoid a "silo policy" approach – and to fully consider the operational context of the University.

### Recommended Action

- Engage the relevant business partners in the review of impacts of click-through services on standard business practices or policies to be consistent and inclusive of operational requirements. (See "Insurance" below for one example.)
- Remove barriers to easy adoption of public sector negotiated agreements, e.g., NET+ and CENIC. (See "Public Sector Agreements" below.)
- Develop a robust information sharing mechanism for vendor assessments. (See "Information Sharing" below.)

### *Insurance*

Policy BFB-BUS-63, Insurance Requirements and Certificates of Insurance requires all contracts or other agreements with suppliers of goods and/or services include:

- A requirement that the supplier maintain certain levels of insurance articulated in the Minimum Insurance Requirements; and
- A requirement that the supplier provide a Certificate of Insurance that indicates that the University is an additional insured.

Exceptions to this policy may be made "under extenuating circumstances" on a case-by-case basis by the local Risk Management Office. The policy recommends that the local Risk Management Office be brought in "early in the contracting process." These minimum requirements are difficult to achieve operationally for click-through services.

### *Public Sector Agreements*

Risks associated with acquiring these services can be mitigated by UC leveraging consortium negotiated master terms and conditions (e.g., Internet2 NET+, CENIC IaaS, federal "Apps.gov" agreements, etc.).

The benefits of the consortium approach include:

- Larger aggregated demand increases the likelihood of attaining appropriate vendor concessions.
- Resources required for contract negotiation process can be contributed by multiple institutions.
- Contract negotiations are conducted once, and then results are leveraged by multiple institutions on an ongoing basis.

The challenges of the consortium approach include:

- Need clarity regarding alignment with UC Purchasing policy (CENIC IaaS is a competitive bidding process, whereas NET+ is not).
- Multiple institutions will be involved, so negotiations will not focus solely on UC's needs.
- To ensure results best meet its needs, UC needs to dedicate staff resources to participate in these consortiums.

### *Information sharing*

As an organization, we lack a comprehensive toolkit and robust information sharing mechanism for completed vendor assessments, including external assessments. A central repository should host all vendor assessments (e.g., AICPA SOC 2 or ISO 27001/2 reports).

The challenges of information sharing include:

- Access to a central repository for vendor assessments.
- Involvement of multiple areas that contribute to assessments, including IT, security, privacy, procurement, counsel and risk management.
- Adequate training on performing security and/or privacy risk assessments.

## 4. ACCEPTANCE OF TERMS

There is a common assumption that zero-dollar click-throughs constitute purchases and require delegation of authority consistent with "Authority to execute purchase contracts, subcontracts, and standard purchase orders for materials, goods, and services to be supplied to the University"[5]. However, this assumption needs to be verified.

Clarity is also needed to understand when a user clicking "I agree" is accepting the terms as an individual and when he or she is accepting terms on behalf of the University. The University of Virginia[6] has developed one approach which transfers the risk to the user.

Ultimately, for click-through terms, there is confusion over who has authority to accept terms and conditions and what they can accept on behalf of the Regents of the University of California. This confusion is compounded by the increased merging of personal and institutional devices (whether laptops, smartphones, or other) and data.

At the same time, it is important to be mindful of distinguishing high risk from low risk circumstances, so that the University can employ effort and attention commensurate with risk. This will maximize the ability of the University community to use of these services and software that are so helpful in University activity.

### Recommended Action

- Extend existing models for low cost procurement delegations to allow low-risk technology purchases to go through quickly using click-through terms.
- Develop guidance on when a click-through is being done on behalf of an individual and when it is being done on behalf of the University.

[5] Delegation of Authority—Execution of Purchase Contracts, Subcontracts, and Standard Purchase Orders for Materials, Goods, and Services to be Supplied to the University.

[6] Policy in draft, available upon request.

# 5. ELECTRONIC COMMUNICATIONS POLICY (ECP) CONFLICTS OR AMBIGUITIES

The privacy provisions of the Electronic Communications Policy (ECP) are intended to protect individual privacy. The ECP protects privacy in the context of the University's values, including academic freedom. This goal remains fundamental to the University, but the underlying privacy model employed by the ECP no longer accounts for the full range of the University's present-day needs. These needs include proactive data protection, a greater range of analytics, and better alignment between the expectations of the University and third-party vendors with whom we increasingly partner.

Specific to the focus of click-through terms, three areas of the ECP have been identified that differ from common current practice by third-party vendors:

- *Consent and Vendor Access*. Click-through services typically require, at time of service provisioning, user acceptance of terms that allow broad vendor access to user content. On the other hand, the ECP intends for user consent to be narrow (for time- and incident-specific access, with an assumption of least perusal to get the job done); and narrowly limits the reasons for which such access is permitted. (Though the "letter of the ECP" may be satisfied by the user giving consent when clicking on "I agree.") Examples of common vendor practices prohibited by the ECP include use of industry standard data loss prevention techniques, monitoring to improve services and develop new ones, and tracking of geolocation data to provide tailored content.
- *Definition of "content"*. The ECP defines content to include transactional information such as email headers and IP address logs. Typically, other organizations provide less protection for such transactional information or consider it public. Click-through vendors may also refer to account information or data aggregated across services as "content", which are not clearly addressed in the ECP.
- *Individual's responsibilities*. While the ECP focuses on the University's actions and impact on the individual, vendor agreements may reflect the impact of an individual's actions on the University or other users. Individuals need to be responsible for recognizing when their use of a vendor's services may be compelling others to consent to unfavorable terms. This is increasingly a privacy consideration with collaborative services: e.g., the tagging of others in Facebook photos, or the ability for users to re-share content shared with them.

## Recommended Action

The three areas described above are part of a larger set of present-day University needs not fully accounted for by the ECP. We recommend UC privacy policies be updated to address discrepancies between vendor and campus standards for privacy drawing on the conceptual framework articulated by the Privacy and Information Security Initiative[7].

[7] See the President's Privacy and Information Security Initiative and a summary of the final report used to present this initiative to the UC Regents.