UNIVERSITY OF CALIFORNIA, BERKELEY

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

AUDIT AND ADVISORY SERVICES
Tel: (510) 642-8292

611 UNIVERSITY HALL #1170
BERKELEY, CALIFORNIA 94720-1170

October 5, 2018

Vice Chancellor Cathy Koshland
Undergraduate Education

Associate Chancellor Khira Griscavage
Chancellor's Office

Vice Chancellor Koshland and Associate Chancellor Griscavage:

We have completed our audit of information and privacy – data usage in online services as per our annual service plan in accordance with the Institute of Internal Auditors' *Standards for the Professional Practice of Internal Auditing* and the University of California Internal Audit Charter.

Our observations with management action plans are expounded upon in the accompanying report. Please destroy all copies of draft reports and related documents. Thank you to the staff of Educational Technology Services and the Campus Privacy Office for their cooperative efforts throughout the audit process. Please do not hesitate to call on Audit and Advisory Services if we can be of further assistance in this or other matters.

Respectfully reported,

Jaime Jue
Interim Director

cc: Associate Vice Chancellor and Chief Information Officer Larry Conrad
Deputy Associate Chancellor and Chief Operating Officer Wanda Ellison Crockett
Associate Chief Information Officer and Director Jenn Stringer
Deputy Director Meggan Levitt
Associate Director Oliver Heyer
Senior Vice President and Chief Compliance and Audit Officer Alexander Bustamante
Assistant Vice Chancellor and Controller Delphine Regalia

AUDIT AND ADVISORY SERVICES

Information Privacy – Data Usage in Online Services Audit Project No. 18-712

October 5, 2018

Reviewed and Approved by:

Prepared by:

Chad Edwards
Auditor-in-Charge

Jaime Jue
Interim Director

University of California, Berkeley
Audit and Advisory Services
Information and Privacy – Data Usage in Online Services

Table of Contents

OVERVIEW

Executive Summary

The purpose of this audit was to assess the current state of governance, risk management practices, and internal control processes related to ensuring the privacy of student data in learning management systems used by the campus.

We conclude that current practices related to the collection and use of student user data in the main campus learning management system (Canvas, locally branded as bCourses) are generally consistent with permitted use by ETS bCourse administrators for purposes of operating the core and expected functionality of the online service.

However, we note an area of emerging risk related to recent requests by some campus units to access individual student data, including metadata on platform usage, to understand the linkage between bCourses usage and individual academic performance. In one case, access to an individual user's platform usage data had been requested by advisors in an academic support unit (the Athletic Study Center) to track student success by individual student and to intervene with counseling or support when deemed necessary.

Management may wish to determine any gaps between the existing Instructure (the provider of the Canvas product) privacy statement and terms of service, other existing campus privacy statements related to web sites and online systems, and the draft systemwide Learning Data Privacy Principles and Practices. These principles and practices also cover areas such as data ownership, the ability to opt-in or opt-out, ethical use, freedom of expression, protection, disposition, rights to access and control. Any such gaps may need to be addressed in an updated campus privacy notice for bCourses.

We note that it is likely, as awareness of the existence and availability of such user metadata becomes more widely understood across the campus, that there will be more individuals interested in student success who will be requesting access to such data for both individual student advising and pedagogical research purposes. As such, the campus would be well served to have privacy values and principles related to the collection and use of such data in place to mitigate the risk of intentional or unintentional practices that would be inconsistent with university and campus policies and practices.

Source and Purpose of the Audit

The purpose of this audit was to assess the current state of governance, risk management practices, and internal control processes related to ensuring the privacy of student data in learning management systems used by the campus.

Scope of the Audit

Based upon our preliminary audit risk assessment, we prioritized our focus on the collection and use of student data in learning management systems and services as an emerging area of risk. As a result, we did not consider as being in scope the collection and use of data related to staff, faculty, and students in their capacity as employees tracked in the campus human resources system (HCM) nor did we include data collected and retained in the PeopleSoft student information system (SIS). Consideration of privacy risk related to these two other systems have been addressed, either directly or indirectly, in prior audits or management reviews.

Our audit planning steps included obtaining an understanding of patterns of current usage of learning management platforms and technologies at comparable institutions, relevant regulatory and operational requirements, and the implementation and use of specific platforms on campus. We note that we also addressed privacy of personally identifiable information more broadly as part of our 2015 audit of the evolving use of cloud computing platforms on campus.

The campus' main learning management system is Canvas (locally branded as bCourses). Canvas is a third-party outsourced and hosted online learning management system provided by Instructure through the campus membership in the Internet2 consortium. Separate instances of Canvas are also used to deliver the School of Public Health's Online Master of Public Health program as well as courses offered by University Extension.

The School of Information has a partnership with 2U for the use of their proprietary learning management platform to support their online Master of Information and Data Sciences and Master of Information and Cybersecurity degree programs.[1]

Our audit fieldwork was conducted between October 2017 and February 2018.

Subsequent Events

Subsequent to the completion of our audit fieldwork, the European Union's General Data Protection Regulation (GDPR) went into effect on May 25, 2018. The Office of the President issued a statement in May stating that compliance, privacy and information functions are working together to develop an effective GDPR compliance program. As such, an evaluation of the design and implementation of such a program was not included as part of the scope this audit.

[1] Given the relative number of students in the Canvas versus U2 platforms, we prioritized focus on the Canvas implementation for our audit. We also note the edX platform, which is a Mass Open Online Course (MOOC) provider, where Berkeley is among 130 providers of course content and materials but does not own or control the underlying learning management system. We did not include the edX platform in the scope of our audit.

Background Information

There are many federal and state laws and regulations as well as internal university policies that relate to information privacy. A summary of requirements is posted at the UC Office of the President's Ethics, Compliance and Audit Services website.[2] In summarizing recent developments related to the topics of the privacy and the collection and use of personally identifiable information, we note three notable events:

1. The four recommendations from the 2013 final report of the UC Privacy and Information Security Steering Committee
2. The 2017 development of a local campus privacy and online monitoring policy
3. The 2017 systemwide development of learning data principles for data in learning management systems

We provide a brief overview of each item below.

1 - UC Privacy and Information Security Steering Committee Final Report (2013)

In June of 2010, President Mark Yudof convened the University of California Privacy and Information Security Steering Committee 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.

In its final report of January 2013, the Steering Committee arrived at four recommendations it believed define an overarching privacy framework that would provide for a systemwide integrated approach to privacy and information security.

RECOMMENDATION 1: *UC Statement of Privacy Values, UC Privacy Principles, and Privacy Balancing Process.*

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

- The **UC Statement of Privacy Values** declares privacy – of both autonomy and information – as an important value of the university, as this is not explicitly done elsewhere; and clarifies that privacy is one of many values and obligations of the university.
- The **UC Privacy Principles** define a set of privacy principles for the university that are derived from, and give concrete guidance about, the Statement of Privacy Values.
- The **Privacy Balancing Process** provides a mechanism for adjudicating between competing values, obligations, and interests, whether as a tool in making policy or to guide decision-making in specific situations, and even in a changing context.

[2] See https://www.ucop.edu/ethics-compliance-audit-services/compliance/privacy/index.html and https://www.ucop.edu/ethics-compliance-audit-services/compliance/privacy/privacy-policies-and-references.html

RECOMMENDATION 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.

RECOMMENDATION 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.

RECOMMENDATION 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.[3]

2 - Berkeley Campus Privacy and Online Monitoring Policy (2017)

In May 2017 the campus adopted a Privacy and Online Monitoring Policy. This campus policy defines requirements for notice, analysis, review, and approval of routine monitoring practices. If monitoring involves electronic communications, the escalation process for non-routine use of monitoring data must meet the requirements of the systemwide Electronic Communications Policy.

The policy requires that campus providers of network and IT systems and services must develop, maintain, and openly publish meaningful notice of their monitoring practices. Meaningful notice requires proportionality to the level of privacy impact – more invasive monitoring practices warrant more conspicuous notice to those individuals being monitored.

3 - Learning Data Principles and Practices (2017)

In summer 2017, concurrent to work conducted by the campus privacy officer, Educational Technology Services (ETS)[4] and similar functions across the system coordinated the development of a draft set of learning data privacy principles and practices, intended as an extension of systemwide privacy values and principles to the specific environment of learning management systems. In this context, learning data is defined to include teaching/learning-related content created by students or instructors including slides, videos, assessments, discussion

[3] With respect to the fourth recommendation, the Berkeley chancellor designated a privacy official although the position became vacant during the course of our audit fieldwork.

[4] The campus sponsors for the initiative are the Vice Chancellor of Undergraduate Education and the Chief Academic Technology Officer and Associate Vice Chancellor for Teaching

prompts, and more. Data can be highly individualized, tracking a student through a specific term/course, or at a meta-level examining large subsets of students or the entire student body population. These draft principles and practices are currently under review by the Office of the President.

Summary Conclusion

We conclude that current practices related to the collection and use of student user data in the main campus learning management system (Canvas, locally branded as bCourses) are generally consistent with permitted use by ETS bCourse administrators for purposes of operating the core and expected functionality of the online service.

However, we note an area of emerging risk related to recent requests by some campus units to access individual student data, including metadata on platform usage, to understand the linkage between bCourses usage and individual academic performance. In one case, access to an individual user's platform usage data has been requested by advisors in an academic support unit (the Athletic Study Center) to track student success by individual student and to intervene with counseling or support when deemed necessary.

This particular usage of personally identifiable information on student platform usage does not appear to be explicitly disclosed in the Instructure (the provider of the Canvas product) privacy notice and therefore management should consider whether a specific and separate bCourses privacy disclosure should be developed by the campus.

Management may also wish to determine any gaps between the existing Instructure privacy statement and terms of service, other existing campus privacy statements related to web sites and online systems, and the draft systemwide Learning Data Privacy Principles and Practices. These principles and practices also cover areas such as data ownership, the ability to opt-in or opt-out, ethical use, freedom of expression, protection, disposition, rights to access and control. Any such gaps may need to be addressed in an updated campus privacy notice for bCourses.

We note that it is likely, as awareness of the existence and availability of such user metadata becomes more widely understood across the campus, that there will be more individuals interested in student success who will request access to such data for both individual student advising and pedagogical research purposes. As such, the campus would be well served to have privacy values and principles related to the collection and use of such data in place to mitigate the risk of intentional or unintentional practices that would be inconsistent with university and campus policies and practices.

SUMMARY OF OBSERVATIONS & MANAGEMENT RESPONSE AND ACTION PLAN

bCourses (Canvas)

Observation

With respect to online learning management systems used on campus, the majority of courses are hosted on the Canvas (bCourses) platform. When logged in to the platform, users are provided a link to Instructure's privacy notice for Canvas as well as their terms of service. These disclosures discuss how Instructure may use user data. However there is no separate campus privacy notice specific to bCourses which would address how the campus uses bCourses user data.

We understand ETS bCourse administrators do not routinely monitor either user activity within a course or session metadata other than to collect and use data strictly for purposes of operating the core and expected functionality of an online service and as such do not conduct online monitoring practices that would be subject to the campus online monitoring policy.

However, some campus units have begun requesting access to student data, including metadata on platform usage, to understand the linkage between bCourses usage and individual academic performance. In some cases, access to an individual user's platform usage data is requested by academic advisors in schools and colleges or academic support units such as the Athletic Study Center to track student success by individual student and to intervene with counseling or support when deemed necessary.

This particular usage of personally identifiable information on student platform usage does not appear to be explicitly disclosed in Instructure's privacy notice and therefore management should consider whether a specific and separate bCourses privacy disclosure should be developed by the campus. Management may also wish to determine any gaps between the existing Instructure privacy statement and terms of service, other existing campus privacy statements related to web sites and online systems, and the draft systemwide Learning Data Privacy Principles and Practices which the campus contributed toward developing. These principles and practices also cover areas such as data ownership, the ability to opt-in or opt-out, ethical use, freedom of expression, protection, disposition, rights to access and control. Any such gaps may need to be addressed in a campus privacy notice for bCourses.

We would categorize this area as an emerging risk for management attention as the awareness across campus of what metadata is being collected is growing but currently only one unit (Athletic Study Center) has advisors that have requested access to such data and only for the student population they serve. Another unit (College of Engineering) has requested access beginning this fall for their student advising staff.

Management Response and Action Plan

Educational Technology Services (ETS) management has reviewed and concurs in general with the findings and recommendations of the audit. It's probably worth noting a few additional details about the overall context for the identified risk. While the Athletic Study Center did initially approach ETS about gaining access to personally identifiable information in bCourses tied to their student cohorts, it should be understood that what is currently provided to the academic advising staff in ASC and the College of Engineering is not a raw data set akin to what a researcher might expect. Instead, the data in question is analyzed, curated, and presented in limited ways via a web application. The application, named BOAC, will be developed further over the next few years to encompass a full range of features in support of academic advisors and student success. BOAC will eventually incorporate a wider array of personally identifiable student information, much of which is already available to advisors in other disparate, locally managed systems. The plan is to release BOAC to the broader UCB academic advising community within the next 1-2 years.

It may also be helpful to unpack and categorize the degrees of risk that the Action Plan might remedy. The risk can be broken out as follows:

1. Lack of transparency: Failure to disclose the use of personally identifiable data, even when the use of the data is for legitimate institutional purposes and where the student may have a limited expectation of privacy or discretion
2. Insufficient controls: Students should probably be given a choice to opt in or out of the usage of the data for specified purposes
3. Violation of law or policy: student data is being shared in likely violation of State, Federal, UC, or campus laws or policies

The steps outlined below are largely aimed at addressing risk in area 1 above.

ETS, in concert with other campus partners, will undertake the following steps to manage the privacy-related risks associated with the use of LMS-derived student data (aka “learning data” or “learner data”) in BOAC:

1. A separate, UCB-specific disclosure notice will be added to bCourses describing the use of student data in BOAC (to be completed no later than October 2018)
2. A communication plan for CoE faculty and students will be drafted in collaboration with CoE advising staff (to be completed no later than October 2018)
3. Meetings with relevant student and faculty representatives/stakeholders will occur over the course of the fall 2018 semester (Academic Affairs VP, Committee on Teaching, Undergraduate and Graduate Councils)
4. BOAC will be put through the Privacy Balancing Process before the conclusion of calendar year 2018.