

# Technology and Privacy on the 21st-Century Campus

Kenneth D. Salomon  
Christopher T. Murray

Technology provides seemingly limitless possibilities in the 21st century, particularly in college and university communities. The Internet supplies information at an unmatched pace: Books can be purchased in less than a minute from a dorm room or while in line at Starbucks; students and professors can stay in contact with their friends and family through social networks; anyone can learn something new from a TED (Technology Entertainment and Design) Talk on their mobile phone while commuting to or across campus; and the lost school mascot can be located via a tracking microchip. However, the increased access and efficiency that information technology provides comes at a cost to personal privacy.

The storage of personal information is of significant concern as we become increasingly reliant on ever-advancing technologies. For example, geolocation tracking services in mobile devices provide an unprecedented means to monitor individuals' movements. Although tracking can ameliorate safety by providing better information to first responders, it can also aid stalkers and criminals in accessing location and behavioral patterns. All three branches of the federal government are actively engaged in defining what information is private in the digital age, how private data should be protected, and how private data can be distributed. As colleges and universities struggle to manage student and employee data, each institution must vigilantly ensure that it collects only appropriate data and that any data collected are securely stored.

## Location Tracking and Biometric Devices on Campus

The University of Illinois (UI) recently signed an annual contract with Rave Mobile Safety (RMS) to provide security services for students, faculty, and staff. Subscribers can opt to receive instant updates on emergency situations on campus through a variety of media including email, text message, campus digital message boards, and even social networking services like Facebook and Twitter. RMS allows UI students to install an application on their phone that opens a one-touch direct line to the police.

The RMS contract also offers UI a Web-based application that ensures that a student makes it from one building on campus to another. With this application, a student can start a timer online and estimate how long it will take to walk to his or her destination; if the timer expires without the student canceling it, the police will be notified and provided identifiable personal information. But there is a catch: these services require students to provide a mobile number or Facebook account, and tracking software must be installed on the student's mobile device. The RMS application raises thorny questions: Who has access to the personal information provided? Can UI disclose or publish this information without student consent and, if so, to whom? Will the information be used to identify or track students without their knowledge?

Privacy concerns go well beyond campus security. New IT, wireless, and mobile technologies enhance student learning,

facilitate administrative functions, protect valuable lab equipment, and safeguard access to dormitories, dining halls, and gyms.

Last fall, Northern Arizona University (NAU) implemented a new attendance radio frequency identification technology (RFID) tracking system to be installed in all classrooms accommodating 50 or more students. Although NAU has embedded RFID tags in student ID cards for several years, the use of the technology for classroom attendance is new. The system reads student ID cards upon classroom entry and generates attendance records for professors. There has been shown to be a high correlation between attendance and student

success, so NAU chose this system to boost attendance. Students argue that attendance tracking systems and the incorporation of those records into final grades would stop them from prioritizing busy schedules.

NAU is not alone in its attempt to boost student attendance through technology. The CreditU system deployed at Stanford University offers rewards. The CreditU app which is currently available for iPhones and under development for Android, was developed by two recent Stanford graduates, Andrew Bellay and Weston McBride. CreditU allows students to register their courses on their phone and gives them electronic tokens for classroom attendance.

Students can redeem tokens for free coffee, discounted food, skipping the lunch line, and even discounts on student loans and car insurance. But use of this app has a cost: to receive tokens, students must check into class using the geolocation services on their phones.

Privacy concerns on campus are not limited to tracking student whereabouts. Many institutions, such as the University of Georgia, use hand-scanning technology to limit access to campus facilities. Arizona State's Biodesign Institute uses iris scanners to access lab equipment. Although reliance on unique biometric signatures can increase both security and efficiency, the



## Are you looking at an unplanned change in your software platform?

UNCERTAIN ABOUT YOUR  
VENDOR AND YOUR FUTURE?

WONDERING ABOUT SUPPORT?

There are significant changes in the Higher Education landscape surrounding Communication Management Software providers. Are you affected?

We're the 'other guys' who have quietly and consistently been providing Communications Management Software and support to Higher Education Institutions for over 28 years.

We live by our core values of:  
Do the Right Thing  
Give the Customer What They Want  
Provide On Going Value

*Perhaps it's time for us to talk!*

For more information contact us at 616.554.0000 or [www.pcr.com](http://www.pcr.com)

*As colleges and universities collect more and more sensitive information, they must take steps to prevent access and misuse both by those inside the campus community and by third parties. Simply stated, 21st century colleges and universities should assume that they are constantly under hacker attack.*

systems require storage of unique personal biometric information and therefore create an opportunity for data to be misused or stolen.

Although students and staff may trust their institution to keep their personal information private, sensitive data are under siege in all corners of our modern society, and protection of such data may ultimately be out of the institution's control. For example, news agencies like News of the World in the United Kingdom have demonstrated that they have the means and ability to use private information nefariously. In addition, leading companies like AT&T and

Sony have been targeted by hackers who accessed large amounts of personal customer data. Colleges and universities have not been immune to data breaches and spills.

#### Data Breaches

"Hactivism" groups like Anonymous and LulzSec have demonstrated that government and private institutions alike are vulnerable to data breaches. Hactivism is generally concerned with privacy, and Anonymous's symbolic use of the bodiless suit and Guy Fawkes mask is a prominent example. LulzSec approaches privacy differently by focusing on security breaches and data dumps for entertainment.

McAfee suspects that China has attempted to access U.S. defense and energy specifications, and the company recently released a report revealing that 49 American organizations had been remotely accessed by computers suspected to be in China. These hackers accessed the Department of Energy and multiple defense contractors, apparently seeking information on U.S. military specifications, satellite communications, and natural gas operations. Many colleges and universities also house vital national energy and defense programs inside their campus communities, making them vulnerable to these attacks as well.

As colleges and universities collect more and more sensitive information, they must take steps to prevent access and misuse both by those inside the campus community and by third parties. Simply stated, colleges and universities should assume that they are constantly under hacker attack in the 21st century. Stanford University Hospital learned from a former patient in August that a breach allowed the medical records of 20,000 emergency room patients to be posted for nearly a year on a commercial website. Individuals' names, diagnosis codes, account numbers, admission and

discharge dates, and billing charges were made public. The university is investigating how the data migrated from its billing contractor to the Student of Fortune website.

In March 2011, the University of South Carolina experienced a breach that exposed the names, addresses, health records, financial data, and Social Security numbers of 31,000 students, faculty, staff, and retirees. The University of Connecticut suffered a similar breach in January.

Malicious third parties are not always the cause of data breaches. Some institutions have had difficulty protecting sensitive, personally identifiable data from unintentional breach. In 2008, a Stanford employee lost a laptop that contained 62,000 current and former Stanford employees' personal information, including Social Security numbers. Last fall, Missouri State University accidentally uploaded the personal information of students, including Social Security numbers, to an unsecured database that was accessible through public search engines like Google.

#### The Courts

A recent court ruling raises concerns about the privacy of admissions information provided to institutions by applicants and parents. The Chicago Tribune sued UI to obtain information on students and their parents in order to write an article about political influence in admissions. In March, a federal judge ruled that the Family Educational Rights and Privacy Act (FERPA) did not prohibit UI from turning over the names and educational records of applicants to the paper, though the release would render UI ineligible for federal funding. The judge's decision was a narrow one, addressing only the question of whether FERPA prohibited UI from releasing the information. In the ruling, the judge held, "Illinois [UI] could choose to reject federal

education money, and the conditions of FERPA along with it, so it cannot be said that FERPA prevents Illinois from doing anything.” Other courts have reached similar conclusions, though some courts have concluded that FERPA is indeed a prohibition.

Although there is a great risk of data breach through illegal or accidental actions, some personal data that institutions collect from students and employees may be disclosed through legal channels, like subpoenas. Many law enforcement officials favor requiring data to be stored for extended periods of time in order to provide future assistance in investigations and potential criminal and civil legal actions. Conversely, privacy organizations urge limited timeframes for data retention in order to minimize intrusion and potential exposure. Colleges and universities must balance their legal obligations to government agencies,

law enforcement, and other stakeholders with the needs and expectations of their students, employees, and alumni to determine how long private data should be retained

#### Legislation and the Administration

Congress and federal agencies have become increasingly concerned with data privacy and security. The past several Congresses have introduced data breach and notification bills, generally in response to a major hacking or data spill incident, but have failed to secure final passage. Once again, in the current Congress, bills are pending in the House and Senate. Yet sending a bill to the president for his signature into law always seems to be one headline-grabbing breach away from passage.

In the meantime, states like California have passed data security and breach notification laws on entities that acquire

and store sensitive personal information about California residents. Institutions that enroll California residents in online courses will collect sensitive personal information about students during the admissions process. Not only must California institutions secure these data and provide notice in the event of a breach, but so too must out-of-state institutions that have online students who live in California. Indeed, all online education providers need to be aware of the data security and breach notification obligations in each state where their online students reside. A national data breach and notification law would greatly ease this multistate compliance burden.

The current Congress and administration have also turned their focus to privacy concerns stemming from the explosion in the use of mobile devices with geolocation functionality. Pending bipartisan bills, such

## Be a Published Author!

Do you secretly long to see your name in print?

Have you ever thought about how impressed your colleagues, your staff, and your boss would be if you had an article published?

Wouldn't that credit look great on your resume?

*The ACUTA Journal* will help you turn these dreams into reality. If your campus has a story to tell, we will see that it gets printed for all the world to see (well, all the ACUTA world anyway).

Call or e-mail editor Pat Scott at 859/278-3338 x221 or [psscott@acuta.org](mailto:psscott@acuta.org). Your next great accomplishment is just a few words away!



as the Geolocation Privacy and Surveillance Act, H.R. 2168 and S. 1212 would protect geolocation information. Yet other proposed legislation seeks to regulate the privacy of consumer online browsing and shopping activities.

The House Subcommittee on Commerce, Manufacturing, and Trade recently approved the SAFE Data Act, H.R. 2577, which would protect consumers from cyberattacks and data breaches. The bill requires companies to notify individuals within 48 hours of a data breach and would establish national standards for data protection. This legislation has been criticized by Congressman Henry Waxman (D-CA), among others, who suggest that it defines “personal information” so strictly that it would not protect information such as photographs and over-the-counter medication purchases. Supporters of the bill argue that it was only intended to protect information like financial data and that general privacy concerns should be addressed through separate legislation.

In the Senate, John McCain (R-AZ) and John Kerry (D-MA) have authored the Commercial Privacy Bill of Rights Act, S. 799. This bill would limit the amount of data that companies could collect from consumers without their express consent, as well as limiting the types of personal information that can be sold. Another effort in the Senate to bolster consumer privacy is Senator Jay Rockefeller’s (D-WV) “Do Not Track” legislation, S. 913, which would allow consumers to opt out of having personal data stored that could later be used for advertising or resale purposes.

Both houses of Congress are seeking to protect consumers’ online and mobile telecommunications activities. However, no

consensus has been reached that delineates what qualifies as personal information to be protected, what protections consumers should have, and whether legislation is necessary.

Against this backdrop, some in Congress, such as Congresswoman Marsha Blackburn (R-TN), argue that self-regulation would be more effective at protecting consumer privacy than would new laws. The corporate sector sees many advantages in the Blackburn approach. On August 30, the Internet Advertising Board (IAB) formally implemented a code of conduct in an effort to demonstrate to Congress that legislation is unnecessary. The code emphasizes consumer empowerment through education and transparency, requiring its members, such as Google, MTV, and The New York Times, to enable consumers to control the collection of their data and to ensure that the data those members collect are secure and anonymous. The Software and Information Industry Association announced on September 1 that it had joined the Future of Privacy Forum’s Application Privacy Working Group (APWG). The APWG is developing voluntary privacy principles and best practices for mobile software apps that will better enable mobile application developers to create and disclose policies to protect personal information. Like the IAB code, the APWG guidelines are intended to demonstrate to Congress that federal legislation is unnecessary. It is too early to evaluate the impact of these efforts on Capitol Hill.

While Congress continues to mull consumer privacy legislation, the Department of Commerce is planning to create a privacy code of conduct. The department intends to hold working groups with privacy advocates and businesses to create a code

that is both flexible and enforceable, while also allowing consumers to feel safe on the Internet. Cameron Kerry, the department’s general counsel, stated in July that a privacy code of conduct would be enforceable by the Federal Trade Commission, which could choose to file an unfair business practice complaint against organizations that chose not to comply with the code.

### Conclusion

As students, faculty, and employees continue to enhance their lives through new technologies, college and university administrators must keep in mind the cost to the privacy of every person on their campus. Geolocation services on mobile phones provide easy contact with the police, but they also can track and store movements. Hacktivism groups steal and dump personal data—some for personal gain or entertainment, and others to raise awareness of privacy concerns.

Institutions should closely monitor privacy legislation and administrative activity, as well as codes of conduct from nongovernmental organizations, and get involved in the debate. Our governments, affiliated businesses, and campus communities must work together so that we all have a clear understanding of what personal information is being recorded, when, for what purposes, and for how long. Participation and engagement by colleges and universities could result in final legislation, rules, and codes that best reflect the needs and responsibilities of institutions and the individuals they serve.

Kenneth Salomon is chair of Dow Lohnes Government Strategies (DLGS) LLC, and a partner in Dow Lohnes, PLLC. Christopher T. Murray is DLGS vice president for education policy. Sean Irving, a DLGS summer intern, substantially contributed to the production of this article.

