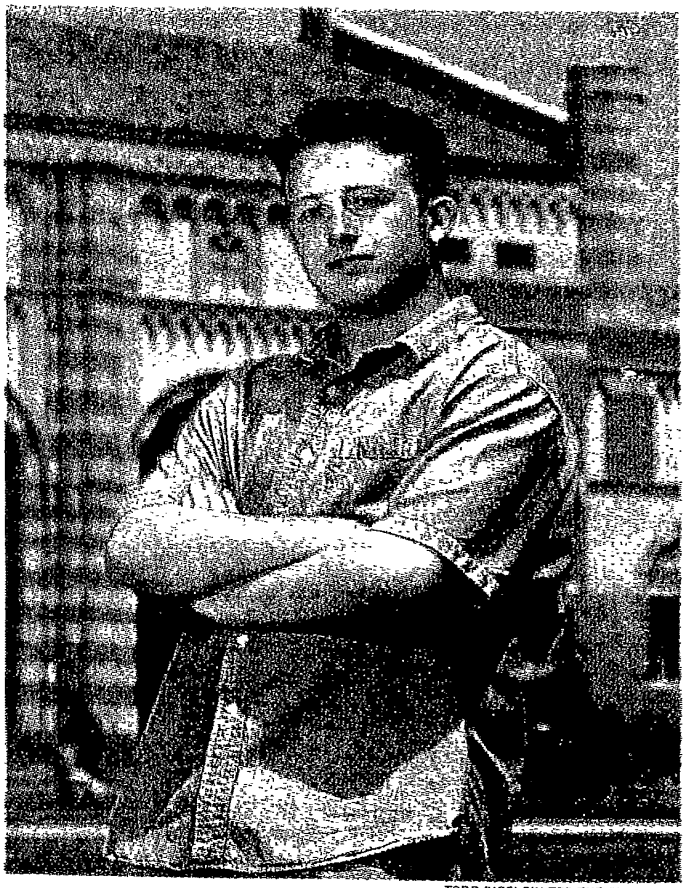
DH20010438E1

The Struggle to Preserve Privacy

Computer networks contain a wealth of student data, but who should see it?

BY ANDREA L. FOSTER



Ryan P. Gutterson, a junior at U.C.L.A.: "As I see it, I don't have any information on campus that really would put me at any risk."

TODD BIGELOW FOR THE CHRONICLE

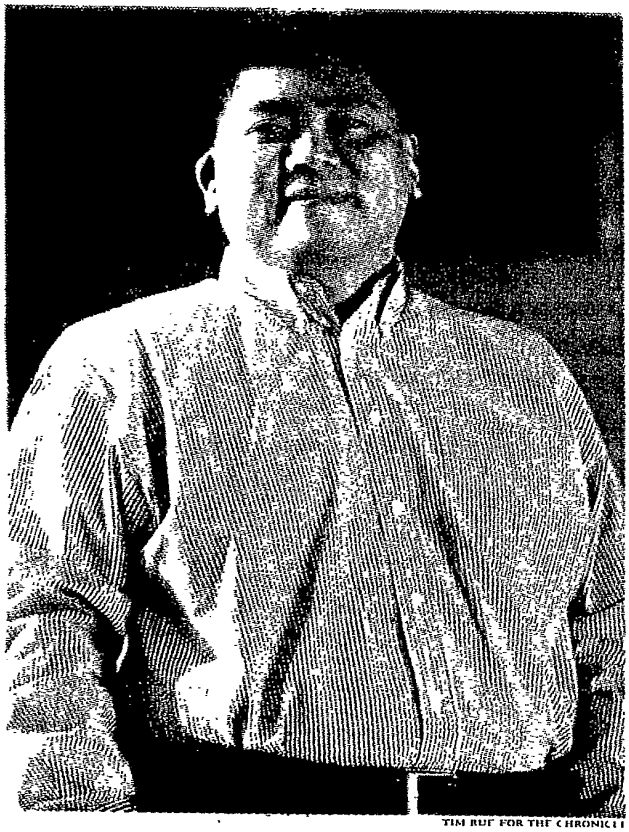
LOS ANGELES

THE UNIVERSITY OF CALIFORNIA at Los Angeles knows a fair amount about Ryan P. Gutterson, a 20-year-old junior. He's from Oakland, Calif. His major is psychology. He has a 3.5 grade-point average and works part time for the university. Mr. Gutterson would readily tell you any of this if you met him at a party, or if you interviewed him for a job.

But U.C.L.A. knows other facts about Mr. Gutterson that he is not so eager to divulge. He has attention-deficit disorder. In his freshman year, paramedics rushed him to a hospital emergency room after he fell off his bicycle while drunk. He is sexually active.

Mr. Gutterson says he is embarrassed by his bicycle accident, and he would prefer that a potential employer not know about his A.D.D. "I would want the chance to explain it to them before they made the assumption that it's a crippling disability," he says. And of his sexual activity he asks, "Who's going to care about that?" But over all, he says, he's not really worried that personal information in U.C.L.A.'s files might fall into the wrong hands or be widely disseminated.

"As I see it, I don't have any information on campus that really would put me at any risk," he explains, while ingesting a fish taco at the Ackerman Student Union. He agreed to make his records available to a *Chronicle* reporter looking at what kinds of personal information U.C.L.A. collects about students, and at the measures the university takes to protect that information, much of which is online. *The Chronicle* chose U.C.L.A. not because the university is perceived as deficient in safeguarding students' privacy, but because it is a large institution that puts a lot of student data online.



Kent J. Wada, who handles security issues involving technology at U.C.L.A.: "People want to know, 'Can I do this? Is this appropriate?' "

TIM RUE FOR THE CHRONICLE

Aware that not everyone shares Mr. Gutterson's nonchalance, U.C.L.A. goes to great lengths to safeguard information it has about students. Electronic records containing students' grades and other private data are protected with passwords and firewalls. Offices that store personal data are locked behind doors opened only with secret numerical codes. Students' identification numbers are different from their Social Security numbers, to prevent impostors from assuming students' identities. And university officials, even when faced with extenuating circumstances like search warrants, aren't allowed to snoop in students' electronic mail on the university's computer network without prior approval from a university vice chancellor.

EVER-EXPANDING COMPLEXITIES

Even with those protections, U.C.L.A. officials struggle to understand the ever-expanding complexities of maintaining students' privacy as they rely increasingly on the Internet to communicate with classmates, sign up for classes, manage their money and their debts, and—in the case of graduate students—electronically record their votes in campus elections.

Officials are not always successful at keeping student data secure, in part because some students treat the information so cavalierly themselves. And the officials

Continued on Following Page

DH>0010438E2

Continued From Preceding Page

say they still depend to a large extent on the trustworthiness of the people handling sensitive data.

The University of California system last fall released an electronic-communications policy that says, in part, "The university does not routinely inspect, monitor, or disclose electronic communications" without first obtaining the communicator's consent. But U C.L.A. administrators have yet to puzzle through the intricacies of that policy.

"People want to know, 'Can I do this? Is this appropriate?' " says Kent J. Wada, information-technology-security coordinator for the university "A lot of times, there is no straightforward answer."

He offers a hypothetical example. A university office creates a Web site for prospective students and wants to keep a log of the pages on the site that they visit most frequently. "You want to be able to do the best you can with the Web site, and yet, should you really be tracking people?" he asks.

Or what about a contract the university might have with an outside company to sell university merchandise online, or to set up electronic mailing lists for the campus? Will the vendor, he wonders, respect the university's privacy policies?

A STEP AHEAD

That U C.L A. is even grappling with how to improve privacy protection in an electronic environment places it a step ahead of most colleges, says Virginia E. Rezmierski, an adjunct associate professor and research investigator at the Gerald R. Ford School of Public Policy at the University of Michigan at Ann Arbor She and a colleague headed a committee that in 1997 released a report recommending how colleges should protect private data. Educause, an academic-technology consortium, created the committee.

The report advocates, among other things, that colleges·

- Notify students about their privacy rights.
- Have policies governing if and when online activity is monitored.
- Inform students about how their data will be used.

When Congress passed the Family Educational Rights and Privacy Act in 1974, the privacy of student records was widely discussed and colleges got busy updating their policies and procedures to comply with the new law Now, says Ms Rezmierski, colleges need to re-examine those polices Colleges want to conduct more of their business electronically, but they need to know about potential pitfalls when data stored in one central system is dispersed throughout the campus, she adds.

Common pitfalls include invasions of privacy caused by ill-informed staff members who don't mean to cause harm Technicians often fail to understand what types of data contain sensitive personal information. And privacy experts frequently fail to comprehend the capabilities of computer technology, says Ms. Rezmierski.

"It will take an incident before they will really come to grips with the vulnerability of the data in these environments," she says of college administrators. "I think it may even take their own personal information being abused in some way."

DAMAGE CAUSED BY A HACKER

Indiana University is a case in point Two months ago, a hacker in Sweden downloaded the names and Social Security numbers of 3,100 students after an employee misconfigured a computer following a hardware crash in January.

U.C.L.A has escaped such disasters Mark C Apodaca, computer-systems manager for the registrar's office, attributes the university's success in fending off hackers to technological protections that he declines to discuss. To do so, he says, could breach security. The registrar's office manages the largest amount of student information.

"No one's been able to do it so far We've had denial-of-service attacks," he says, referring to incidents in which servers are deluged with so many requests for information that they shut down. "But we've never had anyone crack in here yet, and we do the best we can to protect it."

About 1,500 employees on campus have access to the student-information-systems menu, a central database maintained by the registrar's office that lists all the students of the past century The database includes names, addresses, telephone numbers, student-identification numbers, and Social Security numbers. It also lists students' grades, the courses they signed up for, any debts they owe, and whether they have received financial aid.

LIMITS ON ACCESS

Not all staff and faculty members can call up all the information in the database. Access is restricted based on what users need to know Faculty and staff members in academic counseling, for example, typically can retrieve about two-thirds of the information in the database And about 500 people on campus have access to information about a student's financial-aid package They include financial-aid officials and others throughout the university's academic departments who administer money awarded to students

Before anyone views information in the database or on paper, they fill out an application listing what they want to see Mr. Apodaca may then question them about why they want access to certain information Computer-systems administrators within departmental offices also must give their approval before employees have access to student records

Meanwhile, other U.C.L.A. offices forge ahead with their own strategies for handling personal student information The strategies are not uniform or always effective in shielding students' privacy. For example, the university leaves it up to the managers of the numerous computer centers on campus to decide whether to retain files detailing the Web sites students visit.

One of the largest computer centers on campus, the College Library Instructional Computing Commons, does not maintain such files, says Lisa M. Kemp, its manager. But the center tracks who logged in to a particular computer and when. "It allows us to gauge computer usage," she says

Just one floor above the computing commons, in Powell Library, are a number of computers that anyone who enters can use. Although the computers are intended for research, students regularly use the machines to read personal e-mail messages. Unless others are looking over their shoulders, the students remain anonymous.

Similarly, U C.L.A. libraries have no record of what books Mr. Gutterson or other students have checked out and returned. They note only the books students are currently borrowing and whether they owe the library money.

Mr. Wada, the university's information-security coordinator, says that because the library is considered a public facility, tracking users' reading preferences or computer habits would be wrong. "Anonymity is highly prized, so you don't ever introduce a chilling effect on people's desire to learn and to have access to information."

Michele P. Pearson, director of ancillary services for the campus's student-health center, says university officials who manage large amounts of student data are generally responsible about safeguarding it But she adds, "That sense is not generally transmitted throughout the university."

When an advisory group of campus administrators offered money to university offices to test a software product, the health clinic signed up. But the clinic rejected the funds after the technology group decided to split the money between the clinic and another office, so that both could review the product. That would have required sending private medical data from the clinic's computer system to a computer server outside the building, Ms. Pearson explains, a practice she found unacceptable She says of the technology group, "They don't understand the need to *really* protect medical information."

David R. Curry III, manager of audit and advisory services for the university, says keeping private data secure is the duty of chief administrative officers in each department. He and other university auditors check that the departments' policies make sense and include necessary controls. But the responsibility for keeping records private ultimately rests with its employees, on whose trustworthiness the university depends, he says

LOYAL EMPLOYEES

"If I sign a confidentiality agreement and the *[National] Enquirer* shows up with 10 grand, that's where we have a concern," Mr. Curry says. He adds: "One of the things the university has going for it is that we tend to have longtime employees who show loyalty to the institution In a corporate setting the risks are greater."

Even the release of seemingly innocuous data, like students' phone numbers, can put them at risk. When they enroll at the university, students have the option of releasing their phone numbers, along with their residential and e-mail addresses, to be posted on the Web. But university officials say students may not understand how such information could be abused by stalkers or others.

Earlier this month a man convicted of making more than 100 obscene phone calls to female students at U.C L.A. was sentenced to a year in a county jail and three years' probation. Some students said the man, Wallace W. Bouier, obtained the phone numbers from U.C L.A.'s Web site. But Michele Anderson, the deputy city attorney assigned to the case, said she doesn't know how Mr Bouier obtained the phone numbers.

Cases of students being harassed via e-mail are on the rise, according to Tina Oakland, director of the Center for Women and Men at U.C L.A., and Nancy S. Greenstein, who is the head of public information for the U.C L.A. police. "We have seen a trend over the last 10 years of cyberstalking," Ms. Oakland says.

Mr. Gutterson, the Oakland junior—whose address, e-mail address, and phone number are available on the U.C L A. Web site—is not worried. He sometimes uses colleges' online directories to locate friends' phone numbers and addresses, and appreciates that others may need to use the Web to get the same information about him. "While I accept that, yes,

College Policies on Privacy

Colleges have a range of policies establishing when administrators may examine a student's e-mail and other electronic files. Here are excerpts from the policies of five institutions:

Cornell University

"The university reserves the right to limit access to its networks when applicable university policies or codes, contractual obligations, or state or federal laws are violated, but does not monitor or generally restrict the content of material transported across those networks"
(http://www univco cornell edu/policy/RU.html)

University of California System

"The university does not routinely inspect, monitor, or disclose electronic communications without the holder's consent. . When under the circumstances described above the contents of electronic communications must be inspected, monitored, or disclosed without the holder's consent . . such actions must be authorized in advance and in writing by the responsible campus vice chancellor or, for the office of the president, the senior vice president, business and finance."
(http.//www.ucop edu/ucophome/policies/ec/html)

University of Pennsylvania

"While the university does not generally monitor or access the contents of a student's e-mail or computer accounts, it reserves the right to do so However, access to and disclosure of a student's e-mail messages and the contents of his or her computer accounts may only be authorized by any one of the dean of the student's school or his/her designate, the vice provost for university life, or the office of audit and compliance, in consultation with the office of general counsel"

University of Tennessee at Knoxville

"The university does not routinely examine the content of a user's account space; however, it reserves the right to investigate the use of that account and inspect the account contents when deemed necessary."
(http://dii utk edu/moreheadlines/aup/compliance.html)

Wayne State University

"While respecting users' privacy to the fullest extent possible, the university reserves the right to examine any computer files . . No action under this section may be taken by university officers without the approval of the president or his/her designee."
(http://www.dmac.wayne.edu/acceptable_use.html)

SOURCE: CHRONICLE REPORTING

there is a small chance that some crazy stalker could find my number and decide they want to stalk me, I think it's a very convenient service to have, for the most part," he says.

CONVENIENCE VS. PRIVACY

Mr. Gutterson's preference for convenience over privacy also prompted him to provide his parents with his personal-identification number. Students use the number to log on to U.C.L.A. Web sites that pull information from the registrar's student database. The sites allow students to update their addresses, pay their bills, and view their grades, among other things.

Mr. Gutterson says he wants his parents to be able to get on those sites so they can pay his bills. But he also doesn't mind if they peruse his grades online. "I've never got a grade bad enough for me to worry about them getting upset over," he adds. "If I did, chances are that I'm upset about it, too. So I would end up telling them."

University officials say Mr. Gutterson is not unique, and that they can only do so much to safeguard students' privacy when students themselves are unconcerned about it. Literature distributed in the Computing Commons, for instance, warns students to log off the computers when they leave the center. But not every student follows the advice, which means that the next person using the same computer may be able to view the previous user's personal information.

BIRTH CONTROL AND H.I.V. TESTS

Where many students draw the line on sharing information with parents, though, is when specific health concerns are involved. The students worry that parents will find out that they sought birth control advice or had an H.I.V. test, Ms. Pearson says.

Students who visit the health clinic are often asked whether they are sexually active. When Mr. Gutterson visited the clinic in April 1999 complaining of congestion and a sore, itchy throat, he filled out a form that included a question about sexual activity.

Some students fear that students who work in the health center will read their medical records or reveal to others why they used the clinic's services. Ms. Pearson says she dismissed a worker several years ago, after the student revealed to someone the contents of another student's medical chart.

Mr. Gutterson remains unperturbed, even though he has a keener appreciation than many classmates of the importance of keeping records private. His part-time job is updating alumni and donor records.

In his job, he says, he has seen the addresses of several celebrities among the university's alumni and friends. "If someone in my position wanted to be a stalker, they could. But that's why there's an interview process. That's why I have to sign a confidentiality agree-