

February 1996, Vol. 22, No. 4

'THEFT OF IDENTITY' RISES TO THOUSANDS A DAY

Students taking an English course at a junior college in California may have been hoping for "extra credit," but not to the extent they got it.

Their English instructor at Modesto Junior College apparently took the students' names and Social Security numbers off a class list she was issued and opened fraudulent credit-card accounts in their names. Nancy Lee Jones did the same with the SSNs of faculty colleagues, lifted from pay stubs that disappeared from campus mailboxes, according to police.

The college has learned its lesson. This month it decided to delete the first four digits of the Social Security number on class lists in the future. In the fall, it may begin using a randomly selected student ID number.

Jones was arrested Jan. 9 on charges of stealing \$43,000 worth of products through fraudulent accounts set up at American Express, Visa, Spiegel, MasterCard, and elsewhere.

As is usual in the current epidemic of credit-card fraud, the three students and three faculty members discovered the scam when stores or credit-card companies called to see why they weren't paying their bills. "I said I never brought anything at Nordstrom," said one English professor. "The address given on the credit application wasn't mine. It was in San Francisco. But they used my name and my Social Security number." When the man checked his credit report, he found accounts listed for Nordstrom's store, a mail-order clothing company, and two credit-card issuers, all of them false, all of them in delinquency for a total of \$7,000.

The arrest of the part-time English

teacher, who has a Ph.D. degree, did not end the nightmare for the students and faculty members victimized. Each of them had to persuade the three national credit bureaus to delete the fraudulent information from their credit reports - permanently - and to notify credit grantors not to extend credit in their names until the grantors confirmed that the victims themselves were opening the accounts.

Trans Union, one of the three national credit bureaus, is now receiving *1200 calls a day* of this nature, according to its director of fraud victim assistance, Diane Terry. The Modesto
(Continued on page four)

'EVERY STROKE YOU MAKE' MONITORED ON THE INTERNET

By Simson L. Garfinkel

Many users of the Internet are just beginning to realize that their electronic mail might not be as private as the paper mail that it replaces. But few Internet users realize just how little confidentiality has been built into the protocols on which the Internet is based.

Caller ID, which displays the number of an incoming telephone call, has been controversial throughout the nation, but the Internet has had a form of Caller ID from the day that it started operation, with apparently no protests. The Internet's TCP/IP proto-
(Continued on page five)

TRW SELLS ITS CREDIT BUREAU

TRW Information Systems was sold by its Cleveland-based parent company Feb. 9 to Boston investors who are likely to resell it. TRW, with credit reports on 160 million consumers, ranks among the largest two of the three national credit bureaus.

INTERNET (Continued from page one)

col is bidirectional: when your computer connects to another to send electronic mail or to download pages from the World Wide Web, your sending computer transmits its Internet address so that the receiving computer can send back a response. Most UNIX-based servers (UNIX is the most popular operating system for Internet servers) have a command called "netstat," which lists the remote computers that are currently connected to the server.

Once a connection is made, a record of the connection is saved in a log file. A few years ago, only a few programs kept detailed logs of their users. Today, system administrators are encouraged to activate logging for all Internet services. The reason is security: a detailed log file can be used after a break-in to determine how an attacker gained entry, and perhaps even to determine the attacker's identity. A popular program called "tcpwrapper" is freely available on the Internet; it adds logging to programs that do not already have it.

One program that keeps detailed log files is sendmail, the program used by UNIX computers to exchange mail. The sendmail program records in the log files the sender and the recipient of each message, the time it was sent, and its length. These logs are based on the message's *envelope*, rather than its contents. That means that the information cannot be obscured by encrypting the message. The only way to avoid having a return address logged is to send the message through a third-party computer that does not keep logs. Unfortunately, such mailers do not exist. Even the so-called "anonymous remailers" currently operating in Europe, which allow correspondents to reply to each other without knowing each other's identities, keep some records. Last year, in fact, the operator of one such remailer in Finland broke his promise of anonymity and turned over the true name of one of his users to the authorities, who were executing a search warrant from Los Angeles. The alternative, he was told, was forfeiting his computer and divulging the identity of thousands.

Things are even worse on the World Wide

Web. Most web servers keep extensive records of every file that is downloaded, including:

- The name of the file downloaded
- The time that it was downloaded
- The computer to which it was downloaded
- The web browser (e.g. Netscape or Mosaic) that was used.
- The time that the download required
- The web page containing the link that pointed to the page being downloaded.

The Hyper Text Transport Protocol (HTTP) also includes provisions for transmitting the actual e-mail address of the person downloading the page. Today most web browsers don't provide your e-mail address, although this would be a simple matter to add, since it is already stored inside most web browsers (that's how mailto: URLs work). But since many of the companies giving away browsers hope to make their real money by selling servers, this is sure to change, since the people who are buying the servers want the e-mail addresses of people accessing their browsers.

Even without an e-mail address, it's not that hard to figure out where a particular HTTP request comes from, among the millions of computers with access to the Internet. That's because many individual users on the network have their own dedicated Internet Protocol (IP) address. When I worked at MIT Media Lab, my computer had the name daily-bugle.media.mit.edu. I was the only person who used daily-bugle on a daily basis. (This can actually create problems: when an occasional user commandeers a machine for unauthorized use, the actual user can be blamed.)

One of the main uses that companies have found for logging e-mail addresses is to gauge the effectiveness of advertisements that they pay for on other organizations' web sites. Another use is to chart how customers move through a web site. Finally, important information about users can be learned, such as the speed of their network connection and the type of their computer.

A new technology from Netscape called "cookies" has the capability to threaten

privacy even further. This allows a server to download a "cookie" with a secret code into your web browser; at any point in the future, the server can ask your browser if it has the cookie and get it back. This gives web sites an easy way to mark their readers with an indelible marker. Each time you revisit the site, the server will know that it's you. More information about cookies can be found at Netscape's web site, http://www.netscape.com/newsref/std/cookie_spec.html. If you think that these issues are disturbing, then you should realize that all of the trends on the Internet are to *decrease* user privacy, rather than increase it. That's because advertising is emerging as the leading way to pay for all of this expensive Internet technology. Some companies may even give free access to the net, as a way of assuring that customers read their advertisements. The only problem is that effective marketing requires that web sites and advertisers know their customers - and know all about their use of the web site.

IN THE COURTS - Cal. Caller ID

The U.S. Ninth Circuit Court of Appeals has blocked California's attempt to have a higher standard for Caller ID than the Federal Communications Commission's national standard (per-call blocking must be offered as a minimum). The California Public Utilities Commission and several public-interest groups had argued that any unlisted number should automatically be blocked from call display. Pacific Bell and other companies, which had declined to offer Caller ID because of the PUC rule, now say they will offer it by June 1, after a \$40 million public education campaign ordered by the PUC. "A phone number is not among the privacy interests protected by a federal constitutional right to privacy," wrote Judge Arthur Alarcon in a 3-0 decision. *California PUC v. FCC* and *TURN v. FCC*, 94-70197, 95-70470, 95-70519, 95-70591 (9th Cir. Jan. 31).

□ A district court in Northern Virginia on Feb. 6 dismissed a lawsuit by an Arlington man to compel *U.S. News & World Report* to compensate him for its sale of his name and address on a mailing list. Ram Avrahami sued under a state law, similar to those in most states, requiring consent for the

commercial use of one's name, likeness, or persona. The district court judge said that the law seems to authorize a court to stop the commercial use, not to award damages for it, and this exceeds the jurisdiction of the entry-level court. *Avrahami v. U.S. News & World Report*, 95-7479 (Cir. Ct. Arlington Co. Va.). The plaintiff now can argue the issue in Circuit Court, where the magazine has sued for a declaratory judgment that mailing lists are not covered by the law. *U. S. News & World Report v. Avrahami*, 95-1318.

□ The U.S. Supreme Court has let stand a ruling invalidating California's law barring similar landlord-tenant clearinghouses from reporting that a tenant was sued for eviction. A state court last April 26 ruled that the restriction violated the right of free speech. *U.D. Registry v. California*, 95 *Daily Jour.* DAR 5197 (Cal. Ct. App. 4th Div.).

□ Differing from other circuit-court opinions, the 11th Circuit has ruled that police use of a thermal imaging device, which detects heat patterns emerging from a structure, requires a warrant under the Fourth Amendment. In doing so, the court said that heat or sound emissions from a home should be protected as if they were *in the home*, and "activities that take place within the sanctity of the home merit the most exacting Fourth Amendment protections." *U.S. v. Cusumano*, 94-8056, (11th Cir. Oct. 4, 1995).

□ The same court has ruled that Georgia's attorney general was hasty in revoking a job offer because the applicant planned to unite with another woman in a Jewish marriage ceremony. The policy must be examined at trial under the "strict scrutiny" of any state action that restricts religious practices and the right of free association. *Shahar v. Bowers*, 93-9345 (11th Cir. Dec. 20, 1995).

□ The Americans with Disabilities Act prevents a company from demanding that an employee disclose the prescription drugs she takes, a Colorado judge has ruled, adding that the common-law right to privacy does not protect the employee, only the ADA. *Roe v. Cheyenne Mountain Conference Resort*, 95-WY2152-CB (D. Col. Jan. 11). In a separate case in Colorado before the ADA was enacted in 1992, the 10th Circuit Court of Appeals ruled that, as part of a urinalysis test an employee should be required to disclose prescriptions she was taking.