

When it comes to privacy in cyberspace, the average executive is essentially...

Naked

By Pam Baker

Much like the lead character in the fable "The Emperor's New Clothes," the average executive suffers from a degree of delusion when he believes his personal business is fully cloaked.

That's understandable. Because most executives communicate on a personal computer in the sanctity of home or office, the tendency is to assume that the computerized files and various communiques are private. It's difficult to imagine that electronic voyeurs and information gatherers can see all and tell all.

"It used to be that people had to know where to look to find out information on someone, or they had to hire a private investigator," says Wheeler Weber, president of ARCANUM Investigations Inc. in Atlanta. "Now, idle curiosity can be instantly satisfied through a touch of a button (accessing) thousands of Web sites that offer a wealth of personal data."

Where does that information come from? Some of it is gathered or copied by invisible programming that attaches to or invades your hard drive while you are on the Internet. The programs are tiny, digitalized sleuths and saboteurs sneaking across your modem connection at rapid speed and undetectable by you. The industry has given these testy tidbits cutesy names like cookie, applet, punt and lag. But they really spell potential trouble.

A punt or lag is a programmed assault. Both are often thought of only as methods of kicking someone temporarily off the Net — perhaps for some real or imagined offense in

a chat room. But it's not just a simple annoyance resulting in a disconnection from the server. Punts and lags actually give your computer a complex command that overwhelms its resources and suspends its ability to function. And just about any 8-year-old can set them in motion.

Other invasive programs run the gamut, from simple prankster commands to open your CD-drive as a punch line to a harmless joke, to the more sinister password stealers (PWSs), registration crackers, Web trackers, hostile applets and devastating viruses. While you are immediately aware that someone has punted or lagged you, the more serious theft and sleuth programs leave their victims clueless. In any case, your computer's workings are controlled by an intruder.

But information gathering is not restricted to raiding personal or business computer files. Sometimes you give yourself away. You may do it simply by completing a guestbook registration, warranty card, registration form or survey on a Web site.

Or you may be telling all on your own Web site.

"Companies put an incredible amount of information about themselves and their top executives on their Web sites," says Jim Jordan. A partner in the Alston & Bird law firm, Jordan was one of only 110 lawyers in the U.S. selected for the 1999 edition of the *International Who's Who of Internet/E-Commerce Lawyers*, published by Law Business Research. "Sometimes I find out more about my clients on their own Web sites than I do from the information they provide me."

Information gatherers go to great lengths to know you,



ARCANUM's Wheeler Weber: Idle curiosity easy to satisfy.

including monitoring your activities. Cookies, for example, were originally designed as an innocuous form of customer service. These electronic servants track your movements while you're on a specific Web site and then store their embedded information on your hard drive. When you visit that site again, the cookie informs the site of your usual interests. The Web site then immediately turns to pages and presents ads to match your profile. Considering that Web sites can be massive tomes, a cookie is a great time saver and a wonderful new convenience.

Problem is, cookies are normally used without your knowledge and are capable of collecting such personal identifying data as charge card numbers (if you made a previous purchase), your name, address, e-mail address and telephone number.

Once gathered, that information is often sold to a multitude of third parties. A cookie may be very helpful in notifying you of Tom Clancy's latest novel. But it can be harmful if you are running for public office or are up for a promotion, and records of your sudden interest in bankruptcy laws is

*Public records cover
a lot of ground, and many
governments sell their records.*

sold to your employer or to the opposing candidate.

Other electronic monitoring methods are even scarier. Recently consumers learned that if they registered their copy of Windows 98 online, Microsoft could secretly gather their hardware configuration and a specific hardware identifier. While Microsoft claims this was partly an effort to better serve customers and partly an inadvertent action, the effect was to leave user-produced documents tattooed with an identifier code, making anonymity and privacy difficult, if not impossible.

Microsoft has since made a patch-and-removal tool available free to users who wish the identifier removed.

According to the Federal Trade Commission (FTC), 92% of 1,400 Web sites surveyed recently gather information, but only 14% of them disclose their information-collection practices. The FTC (www.ftc.gov) busted megasite Geocities recently for deceptive information-gathering practices under a unique interpretation of false advertising laws.

"The big picture is that there is only a patchwork of laws that address the privacy issue in this advanced age," says Jordan. "Nobody in the U.S. has really taken a blanket approach."

Nor is information gathering limited to private industry. The government is also gathering and releasing information. The federal government, many states and most cities, for instance, sell their public records or provide them free over the Internet. Many of these sites can be accessed by anyone. Some are available only through fee-based services, like KnowX, Information America, CDB Infotek and Lexis-Nexis that have gone to considerable effort to digitalize public records whenever the government is slow to complete the job.

Public records cover a lot of ground, including criminal and civil court cases, bankruptcies, UCC filings, judgments, liens, property records, professional license information, marriage and divorce documents, birth records, Social Security numbers, Department of Motor Vehicle data (including photographs), voter registrations and stock investments, if you own more than 15% of a single company's stock.

What can't be found legitimately is relatively easy to find through a number of other, more questionable information vendors online. Stuff like your medical records, long distance telephone records, banking account number and account balance. It's all there and anyone can take a peek.

Like the fabled emperor, the typical executive is appalled to find he is indeed naked...in public. The initial reaction is to grab some covering by turning to the government to pro-

vide legal protection. But if extensive privacy laws come to be, executives may find this type of cloak too stifling to wear.

Many companies legitimately need information, and such reputable brokers as CDB Infotek, a subsidiary of ChoicePoint, fulfill this need in a timely fashion. Without reliable intelligence, businesses stand to lose billions of dollars to theft, vendor and customer fraud, corporate espionage, employee-generated liabilities, bad investments and pretenders (people who claim to have experience, education and credentials they really do not have).

Laws that cloak the good guys also cover up the bad guys or slow processes designed to minimize risk.

Alpharetta-based ChoicePoint (www.choicepointinc.com) and CDB Infotek (www.cdb.com) largely provide information that was previously gathered from traditional, existing sources. Choking the electronic form does not seal off the information.

*Unfortunately,
cookies
can reveal
such things as
your sudden
interest
in
bankruptcy law.*

"We primarily do the basic due diligence for accounting firms, big lenders, large corporations and attorneys," says Jim Zimbardi, vice president of strategic sales and partnerships at ChoicePoint. "It is fundamentally the same type data search as was done before; now it's just faster and cheaper."

It all sounds so innocuous, but large corporations can go

too far. "Some employers and senior executives become almost information addicts," says Weber. "They want to know everything."

American companies often prefer to use a source like ARCANUM Investigations or ChoicePoint to ensure compliance with existing laws, reduce investigative costs, expedite results and confirm reports.

"Quite frankly, we don't trust a lot of databases out there," says David Cook, vice president of ChoicePoint's Workplace Solutions Division. He cited particular concern with archaic criminal courthouse record systems. The company prefers to collect data itself via field researchers to ensure accurate and up-to-date information.

Cook says ChoicePoint is equally focused on fairness to the individual being investigated and to the investigating company.

"Companies have a legitimate need to know if they are at risk of criminal or fraudulent activity from a potential em-

How the Cookies Crumble: Ways to Protect Yourself

Cookies are killed with applets. So while hostile applets are bad for you, friendly applets protect you. Maybe the applet slogan should be like the National Rifle Association's: "Applets don't hurt you, people do."

You can kill hidden cookies on your hard drive by downloading free or low-cost programs (applets) from such sites as HENSA micros (<http://micros.hensa.ac.uk>), hosted by Lancaster University in the United Kingdom. Available are such programs as No More Cookies for Macintosh and Cookie Pal for Windows 95 and Windows NT 4.0. Select programs according to formats compatible with your computer. Instructions are available on the site.

To cleanse your computer of data collectors beyond cookies, try Cover Your Tracks on the same Web site. The program lets you clear all traces of Web-site visits if you're using Netscape 3.X or 4.X. It clears the pull-down bar, history, cache, cookies and recent documents.

The auto-clearing feature automatically clears once the program has been set, which is a wonderful alternative to constantly running a sweep on manual commands. Cost: \$10.

Killing applets

Generally, it's not a good idea to kill applets. If you do, you can't kill cookies, nor can you use many nifty interactive applications and games. But applets can be bad news, too. To kill most of them, turn off your Java capabilities within browser software like Netscape and Internet Explorer.

To learn more, go to the Georgia Tech Web site at www.gatech.edu, then click on the search link and use the keyword "applets." For more specific information on hostile applets, go to Symantec Security Center at www.symantec.com/avcenter/security/applets/applets.html or the Java Security Hotlist at www.rstcorp.com/javasecurity/applets.html.

Daring souls can check out what all the fuss is about at <http://rucus.ru.ac.za/~soteri/java.html>. Read the warnings carefully before downloading any applets. This adventure is risky. Interestingly, this site was created by the folks at mladue@math.gatech.edu...that is, at Georgia Tech.

ployee, borrower, business partner or vendor," says Cook. "But we also have a responsibility to protect an individual whose life, credit and income may be at stake."

Fees for a ChoicePoint search range from \$15 up to \$150 with a drug screening. Competitor KnowX.com offers many search options for free; fee-based simple searches range from \$.95 to \$6.95 per record, and from \$5 to \$15 per database for detailed records. Information America at www.infoam.com will conduct larger searches for a \$55 a month retainer and a \$.69 per minute connection fee to the database.

Beyond providing assurances in virtually every possible business encounter, ChoicePoint also provides valuable community service, such as a people-locator service for the National Center for Missing and Exploited Children. For the parents of these children, the information literally can be a matter of life and death. Still, abuses do occur and erroneous information can prove devastating to an individual.

"People have been misidentified and found they could not get jobs, credit or even rent an apartment, and they've gone for years without knowing why," says Weber.

So far, the U.S. has tried to encourage businesses to police themselves voluntarily, leading to the formation of self-regulatory efforts like the Online Privacy Alliance (www.privacyalliance.org), Individual Reference Services Group (www.irsg.org), TrustE (www.truste.org), and the Better Business Bureau Online Seal Program (www.bbbonline.org).

Many people, including federal government officials, do not believe these voluntary efforts have done enough to safeguard privacy. The U.S. Department of Commerce is soliciting public comment in an attempt to craft a solution to the problem. Meanwhile, Office of Management and Budget Director Jacob Lew has appointed Peter Swire, a professor of law at Ohio State University and an internationally recognized expert on privacy issues, as the country's first chief counselor for privacy.

There is a hesitancy to regulate the Internet outright, even on privacy issues. Companies and consumers alike distrust

government intervention. Their fears were recently justified when the new European Community Directive on Data Protection became law.

The directive imposes strict restrictions on the use of information gathered from European citizens, even with the citizen's permission. Many U.S. companies today are technically in violation of the law, which is temporarily on hold as Washington struggles to reach a compromise over it. Fortune 500 companies operating internationally now face serious problems in transferring employee records, customer orders, scheduling dockets and other crucial operating data.

In fact, anyone offering goods over the Internet will encounter severe problems if the U.S. does not strike a compromise with the European Union.

"To strictly comply with the European Directive will bring electronic commerce in this country to a standstill," says Jordan.

China also is seeking to control the flow of information over the Internet by restricting access to government-approved servers, who then censor information. It isn't working. Cyber-rebels are flocking to proxy servers, even though penalties are severe. In China's case, at least, the U.S.'s freedom in information may be the best hope for democracy.

So the debate continues. Is the Internet demon or savior? No one seems to know for sure.

In the interim, it's prudent for individuals and companies to protect themselves. Weber advises people to check their

own credit reports every three months and information services once a year to verify their accuracy.

Jordan advises consulting an electronic commerce law firm that has teams of interdisciplinary lawyers before launching a Web site or conducting research on anyone. Some existing laws do apply, and you can get in trouble inadvertently.

"Just owning a Web site can expose you to liabilities in jurisdictions you previously were not subject to," he cautions.

To air your views, contact the U.S. Department of Commerce (www.ntia.doc.gov/ntiahome/privacy) or call your congressman.

Until the dust settles, here's looking at you, kid. □



Jim Jordan: corporate wounds often self-inflicted