Posted on Mon, Sep. 25, 2006

HP scandal reveals world of electronic tracking

ARRAY OF TECHNOLOGIES EXIST FOR DIGITAL SNOOPING

By Dean Takahashi
Mercury News

Hewlett-Packard's investigation into leaks has put the spotlight on electronic tracking technologies that just about anyone can use to try to spy on people.

HP's investigators acknowledged in a memo that they used an electronic ruse to try to trick CNET's News.com journalist Dawn Kawamoto into revealing her sources for stories that included HP's confidential information.

It was just one of a variety of electronic information-gathering tactics that have civil libertarians concerned about how easy it is to use technology either legally or illegally to track someone.

HP CEO Mark Hurd confirmed Friday that HP's investigators used pretexting, or obtaining personal cell phone records by pretending to be the cell phone owners. But technology can be used to track individuals, obtain their passwords, eavesdrop on their wireless networks, or track leaked documents back to certain printers or Word documents.

``It is disturbing to say the least,'' said Katherine Albrecht, director of Caspian, a privacy rights advocacy group and co-author of the book ``Spy Chips.''

``I worry that this is becoming standard operating procedure at companies that have problems with whistleblowers,'' she said.

In a memo sent to HP's top executives by HP ethics chief Kevin Hunsaker, HP said it engaged in a ``covert intelligence gathering operation'' using an untraceable Microsoft Hotmail e-mail account to send a ``legally permissible software-based tracing device in an e-mail attachment sent to Kawamoto.''

Mike Holston, an outside lawyer hired to investigate the matter for HP, acknowledged Friday that HP sent a ``tracer'' to try to discover a journalist's sources. Hurd said he approved the idea of sending misinformation to a journalist, but did not specifically approve the use of a tracer.

Seth Schoen, a staff technologist at the Electronic Frontier Foundation, believes HP planted a ``Web bug'' -- referred to by Holston as a tracer -- on Kawamoto's computer. A Web bug is a link to a graphic image that feeds intelligence back to the sender when the e-mail is opened.

The Web bug apparently was sent to Kawamoto in hopes that she would forward the bogus e-mail, supposedly from an HP insider named Jacob, to her confidential sources. Anyone who received the forwarded message would prompt the return message back to HP. From there, investigators could determine the identity of Kawamoto's sources through their Internet Protocol addresses, or IP numbers.

Kawamoto said in an email to the Mercury News, ``The tactic was designed to work on myself, as well as anyone who received the message and opened the attachment.''

In the case of Kawamoto, the Web bug apparently didn't work, according to Holston.

Richard Smith, a noted privacy advocate and CEO of Boston Software Forensics, said that Web bugs occupy a single pixel on a computer screen and so they are invisible to users.

Some Web bugs have legitimate uses. When someone opens an e-mail with a typical Web bug, it sends a message back to an outside server. The server then downloads an image, such as a company logo, into the e-mail so that the person can see the image. The newest Web browsers or e-mail reader programs have options to prevent Web bugs from working. Often, they prompt the user to answer ``yes'' or ``no'' on whether they want to view the graphic.

By and large, the Web bug is a widely used legal tool, said Kurt Opsahl, staff attorney at the Electronic Frontier Foundation. But Opsahl said under certain situations, the use of a Web bug might be considered under California law to be an ``unfair business practice'' or a violation of false advertising laws if HP used the Web bug to spy on someone, particularly when it espouses a privacy policy that says it doesn't do such things.

``Regardless of whether it is legally defensible, on an ethical level, using Web bugs to track a reporter is troubling,'' said Opsahl.

While Web bugs are relatively benign, there are other, definitely illegal, forms of ``spyware'' that can be embedded onto computers. Those spyware programs, which include ``keyloggers'' that capture typed characters, can be used to discover from afar everything that the target is doing with a computer, said Kevin Mitnick, a security consultant who was once convicted of criminal hacking. While Holston said that HP investigators tailed subjects and went through their trash, he said that no keystrokes were captured and no wiretaps were used.

Laws prohibit the use of such keylogger programs, which are considered the equivalent of wiretaps that require court approval before they can be used by law enforcement. But in some states, the laws haven't kept up with technology. In the European Union, however, even simple devices such as web bugs may be illegal, says Patrick Peterson, vice president of technology at IronPort Systems, a security technology company.

One of the newest means of tracking what someone does with a computer is to eavesdrop on a WiFi wireless network. Such networks typically reach beyond a home's walls to the street, so an investigator in a parked car can watch everything that happens on a WiFi network that doesn't have a secure password.

``If I was a sleazy investigator, I might do this,'' said Smith, the security expert.

Technology is also useful for tracking leaked documents. Microsoft's Word program embeds a serial number in every document, so that document can be traced back to a particular version of Word on a particular computer. In addition, digital ``watermarks'' can be invisibly embedded into documents as well.

Schoen said that the EFF is concerned about how many models of color laser printers -- including those manufactured by HP -- secretly print an identifying mark on every page they print. That mark can be traced to the individual printer, and the Secret Service has used this to track counterfeit currency, Schoen said.

``We are concerned and upset about it and are seeking more information on it,'' Schoen said.

With employees, it takes a matter of seconds to search through a CD of phone records that the phone company sends to large companies along with monthy bills, said Schoen. Hence, it's easy to search for employees who are talking to reporters without authorization.

Robert Holmes, a private investigator in Beverly Hills at IP Cybercrime.com, said that tracking technologies are often used in the work place, since there is usually no disputing that an employer has the right to know what is being done with company-owned computers, cell phones, office phones, and e-mail.

In the future, civil libertarians fear that tracking will become ubiquitous, from the Radio Frequency Identification tags that could replace bar codes to more accurate versions of the Global Positioning Satellite systems -- which track locations -- that are now built into many cell phones.

Mitnick said companies will likely give themselves ``plausible deniability'' by doing as HP did: outsourcing the investigation to contractors.

But in the HP case, the consequences of crossing the line and being overly invasive are clear as the criticism piles up.

Holmes believes that HP'security team used clever tricks in their surveillance of directors, employees and reporters, but he said that to discuss these tactics openly in internal company e-mails was the height of ``amateurism.''

In an ironic twist, HP is a co-sponsor of an award for privacy innovation.

``The company should have consulted its own privacy officer and found out how outrageous these practices are,'' added Beth Givens, spokeswoman for the Privacy Rights Clearninghouse. ``There's irony there.''

Contact Dean Takahashi at dtakahashi@mercurynews.com or (408) 920-5739.