

# Extensive Spying Found At HP

## Feb. Report Sent to 4 Senior Executives

By Ellen Nakashima and Yuki Noguchi  
Wednesday, September 20, 2006; Page D01

The Hewlett-Packard Co. spying effort that has sparked criminal investigations was wide-ranging and included physical surveillance, photographs and spyware sent via e-mail, and it also targeted wives and other relatives of HP board members and reporters, according to a consultant's report prepared for the company.

The Feb. 10 report, obtained by The Washington Post, summarized in eight pages how investigators, to identify an internal leak of confidential HP information, surreptitiously followed HP board member George A. Keyworth II while he was giving a lecture at the University of Colorado. They watched his home in Piedmont, Calif. They used photographs of a reporter to see if the reporter met with him. And they tried to recover a laptop computer stolen from him in Italy so they could analyze its contents.

The report, prepared by a consulting firm in Needham, Mass., hired to investigate leaks to the media, was sent to four HP executives, including HP's ethics director. That suggests that senior HP employees were aware of the spying tactics used as early as February. The report was sent to Kevin Hunsaker, senior counsel and HP ethics director; Frederick P. Adler, an HP information security employee; Vince Nye, a senior investigator; and Anthony Gentilucci, an HP global investigations manager in Boston.

The report, prepared by Security Outsourcing Solutions Inc., detailed extensive efforts it supervised to obtain calling records for home, office and cellphones and fax lines of various HP board members and reporters covering the company.

The report described how investigators sent an e-mail to a reporter for the online technology publication Cnet.com that contained spyware software in an attached file. If opened, the attachment was designed to install itself on her computer and track every keystroke.

The extent to which the Silicon Valley computer company would go to identify the person who spoke anonymously to a reporter about confidential company operations has scandalized corporate America, launched federal and state investigations, and outraged members of Congress, who have called a Sept. 28 hearing on the matter.

Larry Neal, a spokesman for the House Energy and Commerce investigative subcommittee, said yesterday that outgoing HP chairman Patricia C. Dunn, general counsel Ann Baskins and outside

counsel Larry Sonsini are expected to testify. Ronald R. DeLia, owner of Security Outsourcing Solutions and the author of the confidential HP report, is also expected to appear but may choose to invoke his Fifth Amendment right against self-incrimination, said Neal, the deputy staff director for the full committee.

Two others asked to appear before the committee -- Gentilucci, the Boston HP global investigator, and Joseph DePante, owner of a private investigative firm in Florida, have not responded to the committee's request, Neal said.

The House committee has also requested that HP turn over documents related to the investigation and has received "several thousand pages" so far, Neal said.

Another document reviewed by The Post revealed that HP's ethics chief in January was plotting ways to obtain information on board members and was being warned off those tactics by a colleague. On Jan. 28, Hunsaker asked Adler whether there was any way to "lawfully get text message content." Hunsaker wrote about HP board member Thomas Perkins, "Apparently, Perkins almost never uses his cell phone, and instead does just about everything via text message."

In an e-mail reply, Adler told Hunsaker "[e]ven if we could legally obtain the records, which we can't unless we either pay the bill or get consent, I would highly suspect text messaging records are not kept due to volume and expense. The only other means is through real time interception, an avenue not open to us."

HP has conducted two internal leak investigations in the past two years, the first dubbed "Kona 1" and running from March 2005 through the summer of 2005. The second, "Kona 2," ran from January to May 2006, according to sources familiar with the investigation.

Kona 2 was prompted by a story by Cnet reporter Dawn Kawamoto about the firm's long-term strategy, and from the February consultant's report, it is clear that HP focused fairly early -- by mid-February -- on board members Keyworth and Perkins. Keyworth has since admitted to leaking information and resigned from the board.

According to DeLia's report, investigators obtained subscriber information on at least 240 of more than 300 phone numbers sought, and was in the process of analyzing them, including the records of phone calls from Keyworth's New Mexico house, to and from his fax and cellphone, as well as his new wife's home and cellphones. Similarly, the firm obtained records of Perkins's home phone calls from Jan. 4 to Jan. 26, including 12 U.S. calls, three to Britain and two other international calls.

According to the report, board members, reporters and their spouses, particularly at Cnet, were subject to broad background checks, including details of where they worked, attended school and lived. Investigators hired through DeLia's firm obtained call information on Kawamoto's home phone, cellphone and a cellphone believed to belong to Kawamoto's husband's. They conducted "[e]xtensive Media and Internet Content Research" on Cnet reporter Tom Krazit and his wife.

The call information was obtained by a technique sometimes called "pretexting," or impersonating someone else to obtain their phone records, HP said in a Securities and Exchange Commission filing.

The investigators also began an e-mail exchange with Kawamoto "under the pretext of . . . . develop[ing] a dialogue with the reporter." Then, he noted, on Feb. 9, an e-mail was sent to Kawamoto with an attached file with "tracking capability," or software that logs keystrokes in real time.

Investigators experienced in corporate work said the technique, called "keylogging," was out of bounds in this case. "I've been doing this a long time and I've never heard or seen of investigators doing those nefarious types of tactics," said Robert Seiden, president of Fortress Global Investigations Corp. in New York. "To get access to a reporter's computer raises a whole slew of privacy and legal issues."

Kawamoto did not reply to phone messages and a Cnet spokeswoman declined to comment. Krazit also declined to comment.