



## California attorney general says prosecution likely in HP scandal

RACHEL KONRAD  
Associated Press

**SAN FRANCISCO** - California's attorney general said Thursday that Hewlett Packard Co.'s investigation of its own board members violated two California laws related to identity theft and illegal access to computer records.

It's still unclear, however, whether the company or anyone acting on its behalf will face civil or criminal charges stemming from an aggressive investigation to root out the source of leaks to the media, Attorney General Bill Lockyer said.

"The question was, was a crime committed? The answer is yes. Does that mean charges will result? Well, we haven't completed the investigation so we're not yet certain as to who committed the crime," Lockyer said in a phone interview.

"It's likely if evidence continues to come in the way it has that there will be a prosecution," he said. "But we're not ready to go file a complaint. We're still investigating."

The Palo Alto-based computer maker hired an outside firm whose investigators impersonated members of the HP Board of Directors and journalists and called phone companies seeking records of calls placed to and from their home phones.

The company said one board member, George A. Keyworth II, would not be nominated for re-appointment next year because he was a source of the leaks.

Experts in privacy and telecommunications law say HP officials or the private investigators HP hired could face criminal charges. The company could also be liable for civil charges and subject to fines.

Lockyer said no one involved in the investigation is above the law.

"The crime seems to have been committed by the data broker, but that leads to the question of who knew what and when," Lockyer said. "How many others were part of the illegal activity - we don't know the answer to that yet."

People involved in the HP investigation may have also violated a California Civil Code banning a corporation's communication of employee social security numbers to the public.

One of HP's private investigators obtained the last four digits of the social security number of HP director Tom Perkins. The investigator called AT&T and impersonated Perkins, asking AT&T to

send a record of phone calls to and from his house in December 2005 and January 2006 to a free, Web-based e-mail account.

HP spokesman Ryan Donovan declined to comment Thursday on whether HP directors knew in advance that the investigators would pretext. The company has not disclosed which private investigation firm it employed.

"I can't imagine that an investigator imagined the numbers," Lockyer said.

The Securities and Exchange Commission is also reviewing statements HP disclosed after Perkins resigned May 18 in protest over the investigation, SEC spokesman John Heine said Thursday.

The scandal has focused attention on the age-old gumshoe tactic of posing as someone else to access their personal information. Known as "pretexting," the practice often violates state and federal laws, but attorneys and private investigators say it's a commonly accepted practice that lives in a legal - if not ethical - gray area.

Privacy and telecommunications experts say no corporation or individual has ever been charged criminally or civilly with pretexting.

Although the federal Gramm-Leach-Bliley Act prohibits financial institutions from pretexting in most circumstances, investigators not affiliated with banks or other institutions often pretext.

Licensed private investigators in California and many other states are also allowed to employ such strategies to hunt down people who try to hide from the law, said Tamara Thompson, a private investigator in Oakland who has been practicing for 15 years.

"To come out and say no one should be able to get these records under any reason doesn't consider the circumstances under which people benefit from investigators," Thompson said.

Investigators also pretext to find kidnappers or those ordered to forfeit money or property to the court or a winning party in a lawsuit. But the most common use of pretexting is to get phone records of a cheating spouse to present in a divorce case, investigators said.

Joseph Sanscrainte, a telecommunications and privacy attorney at Bryan Cave LLP, said it's impossible to quantify the scope of pretexting. But he said it was "alarmingly easy" to impersonate someone and get detailed call logs e-mailed from a phone company.

"People have actually created a business model out of this," Sanscrainte said.

Pretexting is increasingly drawing the ire of privacy advocates and politicians.

Eleven states have criminalized pretexting since 2005, Sanscrainte said. California's Legislature has considered at least three bills concerning pretexting so far this year, but none has passed.

In May, the Federal Trade Commission filed federal complaints against five e-commerce companies that obtained and sold consumers' confidential telephone records.

HP's liability hinges on numerous factors, attorneys say.

If Lockyer or others want to take the case to court, the company could claim they were not aware that the private investigator was planning to pretext.

"These are smart folks, prudent, and they probably hired a first-class firm - not a guy who breaks into motel rooms," said Ed Harmon, a partner with the Pittsburgh-based law firm Thorp Reed & Armstrong.

Victor Schachter, chairman of Fenwick & West LLP's employment practices group, said HP and the private investigation firm may share liability.

"When you have an outside agency making false pretenses about who they are and why they're calling, it smells," said Schachter, whose firm often employs private investigators. "It's somewhat unknown whether it's illegal, but I'd feel comfortable saying this is very problematic."