

When is spying OK?

Sunday, September 24, 2006

Just how far should you go to find out what is happening behind your back? Should you invade someone else's privacy, if that is what it takes? The Hewlett-Packard Company Board went much too far in its effort to uncover the sources of potentially damaging leaks of corporate information to the media.

The facts are still emerging, but HP reportedly had private detectives follow suspected board members, journalists and others. HP's private investigators apparently tried to install monitoring software on at least one journalist's personal computer. To penetrate the offices of major news organizations, HP may have drawn up plans to plant spies disguised as cleaning or clerical staff.

We know for sure that HP investigators went after confidential phone records of journalists, HP board members and HP employees. You can tell a lot about a person by looking at the dates, times and numbers they call on their personal phones. Maybe you can even find circumstantial evidence of unauthorized disclosures of sensitive corporate information to the press.

Out of respect for privacy, phone service providers are required by law to keep customer phone records confidential. To obtain records on the sly, HP investigators resorted to a notorious kind of fraud. They pretexted. To "pretext" is to pretend to be someone else in order to obtain confidential information or transact unauthorized business, typically over the telephone or online.

Pretexting has become a popular line of work and investigative tool. Privacy advocates are calling for authorities in every state and the federal government to pass additional laws broadly criminalizing pretexting and the sale of personal information obtained by pretexting. HP pretexting targets included George A. (Jay) Keyworth II, a 21-year veteran of the board who resigned over invasions of his privacy and accusations that he had made improper disclosures to journalists. Keyworth defended his press contacts and characterized HP spying as extraordinary: "The invasion of my privacy and that of others was ill-conceived and inconsistent with HP's values."

To help quell controversy over the firm's thoughtless spying, HP chairwoman Patricia Dunn announced that she will step down in January. In an HP press release, Dunn explained the ill-fated investigation, taking some of the blame for the privacy blunders. In a guilty nod to corporate ethics, she admitted that the investigation included "inappropriate techniques." Yet Dunn defended the investigation itself as required to "resolve the persistent disclosure of confidential information" which could "affect not only the stock price of HP but also that of other publicly traded companies."

Dunn has denied that her board had advance knowledge of the investigators' exact methods. So far Dunn has said that her board "was not aware of the tactics its investigators would employ and regrets the pretexting."

But was the board's ignorance willful? Like HP's board chair, some lawyers claim ignorance of the aggressive methods employed by investigators they retain to produce evidence for trial. One study suggests that lawyers number among the most frequent employers of pretexting private investigators. Citing the study, the Washington-based Electronic Privacy Information Center recently concluded in an alert to the American Bar Association that fraudulent pretexting violates the ABA's ethical rules of professional conduct.

Now that business, government and education routinely collect and store volumes of sensitive personal data electronically, pretexting (like its cousin, identity theft) has emerged as a major challenge to honesty. The national scale of the problem may explain why the HP debacle quickly caught the attention of California criminal prosecutors, the Securities and Exchange Commission and Congress.

The U.S. House of Representatives' Committee on Energy and Commerce plans to hold a hearing Friday to get to the bottom of the HP debacle. The committee has asked Dunn, company general counsel Ann Baskins, and outside attorney Larry Sonsini to testify. Anthony Gentilucci, HP's global security manager, has also been asked to appear before the committee, along with private investigators Ronald DeLia and Joe Depante.

HP may have gotten caught with its ethical trousers down because the ethics of investigating suspected misconduct are not clear cut. Trying to find out what is going on behind your back isn't always unethical. It really does depend on the context.

It may be perfectly ethical, for example, for a long-suffering spouse to secretly check up on a husband or wife to confirm suspicions of yet another affair. And it's certainly ethical to monitor young children to make sure they are healthy and safe. Invading privacy to find out what you need to know can be a matter of responsible parenting.

Contemporary parents are even justified in a bit of high-tech spying to investigate what their children are up to. One of my children developed a weight problem that reached medical proportions. I don't permit gorging on junk food, so I wanted to know why a kid who loves ice skating and swimming was 25 pounds overweight. In my school district, parents can log onto a Web site called myschool.account.com and find out exactly what their children have purchased for lunch. Every food item a pupil purchases from funds parents deposit in an account is entered into an electronic log by type, time and date. I now monitor the site regularly, and my little one knows it. Becoming Big Brother of the lunchroom has encouraged healthier food choices by a child with poor nutritional habits.

Corporate responsibility is in one sense like parental responsibility. Parents and corporate leaders both hold the welfare of others gravely in their hands. But the comparison ends there. The folks HP spied on were corporate board members, managers and professional journalists, not children in need of guidance and correction. They are not fit objects of paternalism or authoritarianism. They are fit subjects of privacy protection. They are fellow adults with legitimate expectations of privacy in their conversations and travels, even when suspected of risky behavior or wrongdoing.

Although the financial fates of a multitude can easily rest in the hands of a corporate board, this responsibility alone does not warrant the use of fraudulent and otherwise unethical tactics. The law protects privacy because judges and legislators have recognized the moral significance of personal autonomy and intimacy. Even the government typically must get a warrant or court order before tapping phones or collecting the phone records sought by HP's pretexting private detectives.

HP's board should have shown better judgment in deciding how to resolve the problem of insider leaks to the media. Who knows? A few frank conversations, personnel changes and ethics training might have done the trick.

Anita L. Allen, a University of Pennsylvania professor of law and philosophy, may be reached at moralistcolumn@yahoo.com.