

# Boeing Investigates Employees

posted by PInow.com Staff | November 28th, 2007

Within its bowels, The Boeing Co. holds volumes of proprietary information deemed so valuable that the company has entire teams dedicated to making sure that private information stays private.

One such team, dubbed “enterprise” investigators, has permission to read the private e-mails of employees, follow them and collect video footage or photos of them. Investigators can also secretly watch employee computer screens in real time and reproduce every keystroke a worker makes, the Seattle P-I has learned.

For years, Boeing workers have held suspicions about being surveilled, according to a long history of P-I contact with sources, but at least three people familiar with investigation tactics have recently confirmed them.

One company source said some employees have raised internal inquiries about whether their rights were violated. Sometimes, instead of going to court over a grievance on an investigation, Boeing and the employee reach a financial settlement. The settlement almost always requires people involved to sign non-disclosure agreements, the source said.

Boeing desires to keep investigation details under wraps.

“We will not discuss specifics of internal investigations with the media,” it said in a written response to P-I questions. “Issues that necessitate investigation in order to protect the company’s interests and those of its employees and other stakeholders are handled consistent with all applicable laws.”

But the tactics used by Washington’s largest employer raise questions about where an employee’s rights begin and the employer’s end, and how much leeway any corporation has in investigating an employee if it suspects wrongdoing.

A recent case at another large company highlighted that investigations can go too far. In 2006, a scandal erupted at Hewlett-Packard after the company investigated leaks from its board of directors.

The company was ordered to pay \$14.5 million and to bring its internal investigations into compliance with laws in California, the company’s home state.

The investigation included reviews of internal e-mails and instant messages, the physical surveillance of a board member and at least one journalist, and the illegal use of deception to obtain telephone records of employees and journalists.

For its part, Boeing says that it has multiple internal organizations that provide checks and balances “to ensure these investigations are conducted properly and in accordance with established company and legal guidelines. We do not comment on individual cases or specific investigation activities.”

### **An employee is tailed**

Recently, a Boeing investigator told a Puget Sound-area employee that he was followed off company property to a lunch spot, that investigators had footage of him “coming and going” and that investigators had accessed his personal Gmail account.

The primary reason for the 2007 investigation, the employee said, was Boeing’s suspicion that he had spoken with a member of the media. The employee learned the details of the investigation during a three-hour meeting, in which investigators laid out some of their findings. He has since been fired.

That particular investigation was connected with a July article in the P-I that brought to light Boeing’s struggles complying with a 2002 corporate reform law and cited unnamed sources and internal company documents.

“I wasn’t surprised, but more just disappointed in them, that instead of looking at the problems, instead of investigating that, they investigated the people that were complaining and got rid of them,” said the employee, who had been an auditor in the company’s Office of Internal Governance and asked that he not be named.

“It’s not quite indentured servitude, because you can quit, but when you look at the mortgages and car payments, especially in Seattle, you’re not exactly free,” said the surveilled former employee.

Experts say that tailing employees — though surprising — is usually legal, and that corporations have many options at their disposal to monitor employees. An investigator can do most things short of breaking into someone’s home.

For example, under Washington’s stalking law, licensed private investigators “acting within the capacity of his or her license” are allowed to repeatedly follow a person. Boeing’s internal investigators are exempt under state law from having to obtain a private investigator license, but contracted investigators must hold licenses.

“It’s worse than you can possibly imagine,” said Ed Mierzwinski, consumer program director at the federation of Public Interest Research Groups.

“Employees should understand that the law generally gives employers broad authority to conduct surveillance, whether through e-mail, video cameras or other forms of tracking, including off the job in many cases.”

The law grants companies the right to protect themselves from employees who break the law, such as by embezzling money or using the company warehouse to run a drug-smuggling ring.

The problem, Mierzwinski said, is when companies use the surveillance tactics available to them to root out whistle-blowers.

“We need greater whistle-blower protections,” he said. But, “if you’re using the company’s resources and you think it’s protected because you’re using Hotmail, think again.”

Privacy laws ask whether a reasonable person would be outraged by a particular act; reasonableness is an oft-cited concept in law, explained Bill Covington, a University of Washington professor on technology law and public policy. Washington is a “will-to-work” state, meaning employees can be fired without reason, he added.

“We cannot write laws that cover every circumstance,” he said. “A jury can apply a community standard of what they deem to be fair and right. There are just too many other situations.”

Unfortunately, the public itself does not know what it wants, he said.

“I don’t think we have made up our mind which way we want to go with these particular laws,” Covington said. “You are having a classic clash between business ... and privacy groups.”

### **You are being watched**

So when does privacy begin? When an employee steps across the threshold into his or her own home, experts say.

“The only thing your boss can’t do is listen to personal telephone calls; that’s covered by wiretapping laws,” said Lewis Maltby, president of the National Workrights Institute in Princeton, N.J.

Companies following workers typically do so to check on the legitimacy of workers’ compensation claims. A company needs to know if a worker who claims injury is actually mowing his lawn, Maltby said. It is “completely inappropriate” to trail employees to see if they are talking to reporters, he added — but it is legal.

As one expert at the American Civil Liberties Union pointed out, just as the average Joe could trail his neighbor if he wanted to, companies are allowed to trail employees.

“I can’t harass the person, but there’s nothing that prevents me from just following him,” said Doug Klunder, privacy project director at the ACLU of Washington.

Klunder said that reading private e-mails is “highly questionable.” Companies should be able to know that employees are checking e-mail, but should not be able to view the contents of the e-mails.

“We certainly don’t believe that an employer should be able to read private e-mail content just because it’s accessed on a work computer,” he said.

However, “it’s a tricky area because there aren’t a lot of legal protections in Washington and in most states where we have employment-at-will. There are some privacy rights of employees, but they are limited relative to the employer.”

When Boeing employees sign on to the company network, a screen pops up to tell them that “to the extent permitted by law, system use and information may be monitored, recorded or disclosed and that using the system constitutes user consent to do so,” according to Boeing.

### **Rights for whistle-blowers**

If a corporate investigation discovers employee wrongdoing that merits discipline or dismissal, workers have little recourse, experts say. Whistle-blowers, on the other hand, are afforded more protection, but only if an investigation is deemed retaliatory.

“There are no employee rights. Employees have little negotiating power,” said Bill Mateja, former point man for President Bush’s Corporate Fraud Task Force, formed in 2002. “Only if they’re in the position of whistle-blower do they have a little more oomph.”

Whistle-blower cases can be dismissed for many reasons — the employee might not have understood the law, or the employer’s retaliation is not severe enough to merit fault, “or it can be that the investigation cannot prove that the adverse action was taken for the reason that was complained about,” said David Mahlum, assistant regional administrator for Region 10 of the Occupational Safety and Health Administration. That agency investigates whistle-blower complaints.

Robert Ellis Smith, a lawyer and the publisher of Privacy Journal, a monthly newsletter, called whistle-blower protections the “wild card” in employee protections.

“Protections against electronic surveillance are virtually non-existent in the workplace,” Smith said. “The one wild card for this is federal protections for whistle-blowers. Aside from that, the privacy laws are quite weak.”