



Boston Concord Hanover Manchester



Brian D. Thomas
Direct dial: 603.627.8136
Fax: 603.641.2399
bthomas@sheehan.com

Practice Areas

Business Litigation
Intellectual Property and
Technology

Additional information for this attorney
may be found on our website.

Good Company

Spyware: A Growing Threat to Businesses and Other Organizations

Thursday, January 31, 2008

Most businesses have electronic system policies that regulate computer usage by their employees. Few businesses, however, address the computer monitoring software known as spyware. Once installed on a computer, spyware gathers and reports information about the end-user. Although many types of spyware exist, of particular concern to businesses are those spyware programs that are surreptitiously installed on a computer to intercept emails, display screens, keystrokes and to access other confidential information. This article describes both the growing threat of these programs and the legal system's response to it.

Failure to eliminate spyware in the business setting could result in the capture and misappropriation of sensitive business information or worse, the dissemination of that information to the public. Indeed, a federal district court in Ohio recently held that private information unlawfully obtained through the use of spyware may be introduced as evidence in a public judicial proceeding.

I. *Potter v. Havlicek*

The *Potter* decision arose from a separate but related divorce proceeding in Ohio state court. The husband alleged that his wife was involved in an extramarital affair with the plaintiff, Christina Potter. The husband installed spyware on the family computer that both he and his wife used, enabling him to intercept copies of email and text message communications between his wife, Amy, and Ms. Potter. The husband later announced that he planned to submit the intercepted communications to the state court as part of his divorce proceedings.

Upon learning that the husband had intercepted the private communications, Ms. Potter filed suit in federal court under the Electronic Communications Protection Act (the "ECPA"), seeking an injunction barring the husband from presenting those communications in the state court divorce proceeding. Among other things, the ECPA prohibits the unauthorized interception of wire, oral and electronic communications. The ECPA's so-called "suppression provision" also provides that certain unlawfully obtained communications may not be received in evidence in any trial, hearing or other proceeding before any court.

The federal court in *Potter* recognized that the husband's use of spyware likely violated the ECPA but held that the suppression provision only applies to wire and oral communications, not electronic ones. Therefore, the court refused to bar the husband from using the spyware-intercepted electronic communications in the public divorce proceeding, despite the



Boston

Concord

Hanover

Manchester

fact that the evidence was unlawfully obtained. The court did warn that the disclosure of Ms. Potter's private communications in state court may be actionable civilly or criminally, but concluded it did not have the authority to forbid such disclosure.

II. Message to Businesses and Other Organizations

The events in *Potter v. Havlicek* arose in a non-business dispute, but the decision should nevertheless serve as a warning to employers nationwide: if an employee transmits an electronic communication containing sensitive business information, and that communication is unlawfully intercepted through the use of spyware, that information may involuntarily enter the public realm in a related judicial proceeding. This is especially significant for companies with employees who work remotely out of home offices, where the employee's family or friends may share access to the company computer. In that situation, it is possible that a non-employee may utilize spyware to intercept communications containing sensitive business information belonging to the employer. While the ECPA makes it illegal for the non-employee to do so, it does not keep the improperly intercepted communications out of the public realm if that information later becomes part of a lawsuit or other judicial proceeding.

At the very least, employers must tighten their electronic systems policies to address the threats posed by spyware, and take steps to eliminate situations in which an employee's communications may be intercepted. This includes rigorous limits on the use of company computers, safeguards to prevent the unauthorized use of the employer's system and hardware by non-employees (even family members), and steadfast enforcement of all such restrictions.

Likewise, spyware presents profound challenges for colleges, universities and other internet service providers. For example, universities have statutory obligations to protect the privacy of student-identifiable information. Spyware creates potentially alarming holes in the colleges' and universities' abilities to carry out these important duties, such as those under the Federal Family Educational Rights and Privacy Act (FERPA), by providing third-parties, not unlike the husband in *Potter*, with access to mountains of private information. Service providers must educate their user base in these circumstances and, at a minimum, prohibit the installation and use of spyware, even on privately owned computers. The first step is a comprehensive, coherent policy aimed at advising all users of the system that spyware poses real risks to them.

This article is intended to serve as a summary of the issues outlined herein. While it may include some general guidance, it is not intended as, nor is it a substitute for, legal advice. Your receipt of Good Company or any of its individual articles does not create an attorney-client relationship between you and Sheehan Phinney Bass + Green or the Sheehan Phinney Capitol Group. The opinions expressed in Good Company are those of the authors of the specific articles.