Shook, Hardy & Bacon L.L.P.

national employment PERSPECTIVE

NOVEMBER 4, 2010

A PUBLICATION OF SHOOK, HARDY & BACON L.L.P

FOCUS ON POLICY

SHB's National Employment & Policy Practice Represents Corporate Employers Exclusively

SEVENTH CIRCUIT DECISION SERVES AS A REMINDER TO EMPLOYERS TO REGULARLY UPDATE TECHNOLOGY POLICIES

This Newsletter is prepared by Shook, Hardy & Bacon's National Employment Litigation & Policy Group[sm]. Contributors to this issue: Bill Martucci, Mike Barnett and Jennifer Oldvader.

Contact us by e-mail to request additional documentation or unsubscribe.

Attorneys in the Employment Litigation & Policy Practice represent corporate employers throughout the United States in all types of employment matters. To learn more about the SHB employment group and its members, see SHB.com.

The Seventh Circuit Court of Appeals recently provided yet another reminder to employers that they must regularly review their technology and computer-use policies in an effort to keep pace with rapidly changing laws concerning electronic monitoring and privacy—as well as the even more rapidly changing technology itself.

The case is *U.S. v. Szymuszkiewicz*, No. 07-CR-171 (7th Cir. Sept. 9, 2010), a criminal matter in which Szymuszkiewicz, an IRS agent, had set up a "rule" in Microsoft Outlook that directed the program to forward a copy to him of all messages received by his supervisor. He was convicted under the federal Wiretap Act, which broadly prohibits the intentional interception of wire and electronic communications without consent. *See* 18 U.S.C. § 2510 *et seq*.

In his defense, Szymuszkiewicz argued that he did not violate the Wiretap Act because he did not "intercept" any "electronic communication" while the message was "in flight." Because he merely forwarded e-mails that had already arrived at his supervisor's computer, he argued, no "interception" occurred. According to Szymuszkiewicz, his conduct (at worst) violated the Stored Communications Act.

Szymuszkiewicz's defense, which the Seventh Circuit rejected, demonstrates the lack of clarity surrounding the proper application of the Wiretap Act to modern-day technology and the effect of the law on today's workplace. Indeed, courts have struggled with how to apply the law—originally written to cover landline telephones—to new technology, including e-mail, Voice over Internet Protocol [VOIP] calling and cell phone technology.

Szymuszkiewicz provides guidance on these issues and raises red flags for employers. According to the court, accessing voicemail and e-mail messages without proper consent can create civil and criminal liability under the Act.

The court found that the Wiretap Act does not require “in flight” interception. Writing for the court, Judge Frank Easterbrook noted, “[t]here is no timing requirement in the Wiretap Act, and judges ought not add to statutory definitions.” The court also relied heavily on the transformation in technology that has occurred since 1968.

In short, phone calls in 1968 occurred over a single circuit, which could be “tapped” and listened in on by another person. Today, such things as e-mails, VOIP communications, and some cell phones rely on the transfer of “packets” (segments of a message) to transfer voice or data. These packets of information travel over different routes, at different times, and are reassembled at the server. The court is clear in its opinion that the Wiretap Act must be able to apply to new technology like packet transfers. The result, acknowledged by the court, is that the Wiretap Act and Stored Communications Act overlap, and liability can exist under both for the same activity.

The practical effect of the court’s ruling is that employers must be cautious in monitoring their employee’s electronic activities, or face possible liability under both the Wiretap Act and Stored Communications Act. Indeed, the Seventh Circuit explained that, in addition to e-mail, listening to voicemail without the consent of either party involved would constitute an unlawful interception. In dicta (and counter to other circuit opinions), the court indicated that this would be the case even after a message “sits” on the system.

Both the Wiretap Act and Stored Communications Act, however, provide a fail safe for employers: consent. 18 U.S.C. § 2511(2)(d); 18 U.S.C. § 2701 (c). Employers must ensure that (1) employees—current and former—actually or impliedly consent to any monitoring of their communication (whether phone, messaging system or Internet communications) through the company’s electronic resources policy or other notices; and (2) human resource professionals know they cannot access any of these systems as part of an investigation without proper consent.

A good approach moving forward is to ensure that electronic resource polices explicitly cover potential monitoring of all company technology systems, including e-mail systems and voicemail. An even safer approach would be for employees to sign an acknowledgment concerning monitoring.