

## **When Employees Surf, Companies Face Risk**

*Monday, March 14, 2011*

Matt Chandler

When someone chooses to Tweet, Skype, Facebook or surf the Web on company time, possibly with company equipment, does it open up employers to legal liability down the road? Yes, say area attorneys.

Whether you have a payroll of two or 2,000, holding employees accountable for their technology use can mean the difference between maintaining a productive, efficient workplace or ending up on the short end of a lawsuit.

Attorney Lisa Coppola assists employers looking to establish policies in a variety of areas, including issues related to social media and technology. She is a partner in Rupp Baase Pfalzgraf Cunningham & Coppola LLC.

"We work a lot with companies to prevent risks from occurring in the first place," she said. "We work with our clients to make sure their policies are fair for the employees but also protect the interests of the company."

The problem is too many companies lack a formal employee handbook with clearly defined policies.

"It's very common to see companies that aren't keeping up with these issues of technology like they need to be," Coppola said "Now part of the dialogue when we talk to our clients is certainly, 'We have to address this somehow.'" "When it comes to technology issues, employers can minimize their liability by being proactive.

"Risk is very much viewed under the law in a continuum," she said. "So a lot of times what we will see is that if a company addresses an issue in a handbook, then it gets a presumption in the law that it has done the right thing. Then, if in this case an employee does something in violation of that handbook, the policies can protect the employer."

In addition to establishing policies, employers can utilize outside companies to monitor employee use of technology. James Domres is COO of DIGITS LLC, one such company. He brought more than 30 years of experience as a member of the state attorney general's office to his job as a forensic technology investigator. And he says that similar to the handbook issue, companies too often play catch-up when it comes to dealing with employees and technology.

"When our clients come to us, it is usually with a five-alarm fire," Domres said. "Some of that is because they don't think of some of these things before problems arise. They may have written policies for different types of technology and media, but in many cases they haven't looked at them since they wrote them."

There are several key questions he asks employers: Do you want your people using social media or not? Do you want to allow them to go to their Gmail account or do you want to focus strictly on a hard-line policy?

From there, Domres said his company can identify everything from what websites an employee has visited to every e-mail they have sent or received (even the deleted ones). By recovering all of the information from the hard drive of a company computer or Blackberry, Digits can provide an employer ammunition to back up the termination of an employee or fight litigation arising from a claim of wrongful termination.

"Sometimes companies think if they have a firewall in place, that solves their problems as far as the Internet goes," he said. "We tell them that if you Google 'How do I defeat the company firewall?' you'll get about 20,000 ways to get around it."

Domres offered companies some advice: Audit and review your policies annually and make sure you are offering a refresher course to employees.

"What we preach is a policy to audit," he said. "What a lot of companies don't do is hire somebody or have a forensic component within their company to go by and take a random look (at what employees are doing online). "Companies may say they can't constantly look over employees shoulders and monitor what they are doing. You don't have to monitor, as long as the threat to audit is there. It accomplishes the same thing."

Elizabeth Carlson, meanwhile, is an attorney with Hodgson Russ LLP who specializes in advising her business clients on matters related to social media and technology. She said the chance of compromising private information and confidential company material greatly increases with employees visiting outside, unauthorized sites.

"For all of our health-care clients, there are issues of information protected by HIIPA. For our school district clients, there is student information that is confidential," she said. "Those are all issues that are of concern, and I think you also have to look at the fact that as the social media networks are being used by more employees, more information is out there that can be potentially electronically stored information, as defined by the federal rules. And accordingly, that information would be discoverable."

Translation: When litigation arises, opposing counsel may uncover the history of an employee and open up his or her company to bad things.

Carlson said for many employers, the challenge comes from not knowing exactly what they can and should be doing to protect themselves.

"At this point, I don't think the case law has necessarily caught up with the technology," she said.

Sean Beiter, partner in Goldberg Segalla LLP, agrees that advances in technology and an increasing number of employees using it can make employers vulnerable.

"One of the first things it manifested into was an uptick in harassment claims based on two things," Beiter said. "Individuals viewing adult websites while at work and someone else seeing it, or people forwarding an e-mail that had adult content in it, creating a hostile work environment."

According to Beiter, harassment claims had waned with the increased awareness that employees weren't supposed to have questionable posters, calendars and other materials in the workplace. That all changed with the technology revolution. "Somehow, the easy access to this material on the Internet gave some people the idea that it was OK, " he said. "I also think it is sometimes the case of individuals who wouldn't think of accessing this type of material from home, so they do it from the workplace."

Whether it's employees cheating the company out of productive time while surfing the Web, potentially allowing access to proprietary company information or inviting computer viruses and creating the potential for harassment or lawsuits from viewing pornography on work computers (A recent study found that as many as one in three employees have visited adult websites from their work computer), what is the bottom line for employers looking to protect themselves?

"Employers need to monitor their employees' activities in regard to their use of the Internet, including the use of social media sites," Beiter said. "For that to be effective, employers need to regularly remind their employees: 'We have the capability to monitor your Internet usage and we are doing so.' "