The Liabilities of Social Networking Websites

by J. Craig Williams

Social networking sites are likely something your children and perhaps some other tech-savvy professionals may have introduced to you. If not, buckle up, it's likely to be a rough ride if your law firm or company dives in without testing the water first.

The leading sites are Facebook, MySpace, Classmates.com and LinkedIn. The latter has more interest for professionals, but there are also internal corporate networking sites, and instant messaging.

Each site is designed to increase communication among its users, and law firms, corporations and others are using the sites to increase communication between professionals and corporate employees. Social networking allows employees faster communication with one another. Sometimes, however, there can be a downside to opening communication *via* the Internet.

Let's look at a few examples together with their corresponding solutions.

Potential legal liability.

There's been a rash of students libeling and slandering their teachers online, and in some instances threatening the teachers to the point they can't work. If employees were to use corporate IT resources for similar purposes, then the company could be held responsible in any ensuing litigation.

The solution?

Monitoring employee usage of the Internet can be accomplished through keystroke and screen logging programs, but they generally work best on a single workstation basis; otherwise monitoring the monitors can become a job in itself. It's best to adopt a computer use policy. Most technology lawyers can create such polices to address various corporate structures and potential uses.

Virus Exposure.

Social networking sites are open to users and do not generally restrict the input of content or links. Remember that security is not the site's focus – it's designed to increase communication. Most networks have the potential to unwittingly

introduce malware, viruses, worms and spyware to your corporate network.

The solution?

Install hardware and software firewalls, and establish a corporate-wide policy against downloading any software without permission from the IT department or outside consultant. If you have only a virus-scanning software program installed, you're very vulnerable.

Decreased employee productivity.

There's a fine line between networking for business and networking for personal purposes. Personal social networking at work decreases employee production. In fact, a Goldman Sachs trader in the U.K. was spending four work hours a day on Facebook. When he was told to stop, he posted the warning e-mail and wrote, "It's a measure of how warped I've become that, not only am I surprisingly proud of this, but losing my job worries me far less than losing Facebook."

The solution?

Limit at-work use of social networking sites to those employees who have legitimate reasons to establish networks. Obvious users are sales, marketing and rainmakers. Once these limits are established, then also limit the daytime access to social networking sites.

Trade secrets.

Allowing employees to use company computers in an open-networking format may allow the site to download software to invade your system. Even if you can stop an invasion, then your employee may be the problem in allowing company secrets to leak out, either inadvertently or by mistake.

The solution?

Establish corporate policies about the disclosure of client or customer information, and lockdown private information such as social security numbers and other personal information. Develop a corporate policy ahead of time to notify customers or clients if a breach occurs. Most technology lawyers can readily create such policies and make recommendations to remedy the situation. California Civil Code section 1798, the Information Practices Act, along with the California Financial Code and other federal privacy laws limit the dissemination of personal, private information and set forth fines and penalties for violations.

Bandwidth.

Most of these sites allow users to upload music, pictures and videos, including high-definition movies and other large files. Allowing employees to download and upload files can slow your network down to a crawl.

The solution?

Prohibit file sharing of music or videos, and keep picture uploads to a bare minimum.

Copyright violation.

Users who upload movies and music may violate copyrights. By allowing employees to violate these copyrights, the company may be contributing to the violation of multiple copyrights independently exposing the company to liability.

The solution?

Adopt a policy prohibiting copyright violations and enforce it.

Buy-in.

Social networking sites claim its use will increase connections and, consequently, sales. While mid-level employees may buy into the sites, top-level executives have extensive personal networks and do not rely on technology.

The solution?

Time. As the Internet becomes more ubiquitous among management and upper management, social networking will reach further into the company and its computers. As Internet users become older, social networking will become more computer-oriented and far less personal.

J. Craig Williams is a cutting-edge technology law lawyer in Newport Beach who, despite using computers and social networking sites, still appreciates face-to-face meetings and handshakes. His new book, How to Get Sued, published by Kaplan Publishing, comes out in early June.