

## WHY IT PAYS TO HAVE A NETWORK POLICY FOR YOUR COMPANY

When used appropriately, Email, voicemail and the Internet can eliminate borders of time and space, making it possible for us to do more with more people and businesses. Used inappropriately, they can put companies at risk, both financially and legally. The key to optimizing the former and minimizing the latter? An effective network usage policy.

In today's high technology, communications-driven workplace, the HR professional faces complex challenges that transcend hiring and benefits administration. Workstations fitted with telephones, fax access, Email, and Internet access to the Worldwide Web, provide today's skilled knowledge worker with the tools to be more efficient and productive than ever before. Unfortunately, this same "tool-kit for productivity" also offers a host of new opportunities for abuse and the potential for litigation liability.

How significant is the problem? Very significant. Whether misuse manifests itself in the form of various types of employee lawsuits (i.e., sexual harassment as a result of objectionable Internet material being downloaded and/or displayed) or in lost productivity, the potential is real.

### **Consider these statistics:**

- Sexual harassment complaints filed with the Federal Equal Employment Opportunity Commission jumped from 10,532 in 1992 to 15,618 in 1998 - nearly a 50 percent increase.[i].
- Payouts - not including private settlements - rose 170 percent, from \$12.7 million to \$34.3 million.[ii].
- In one month alone, 22.8 million Americans used Web sites on company time.[iii]
- A single diversion, stock trading, led 8.2 million people to visit Yahoo Finance, CBS Marketwatch, Schwab, E\*Trade and other financial sites at work, up from 6 million just three months before.[iv]
- About 25 percent of all corporate Internet traffic, much of it surreptitious, is considered unrelated to work.[v]
- Long-distance charges total about \$100 billion a year and only half of that is business related. xperts say anywhere from 10 to 30 percent is unreimbursed personal long-distance calls.[vi]

Whether employees are surfing to sexually explicit Internet sites, trading stocks online, Emailing or calling friends, it all adds up to one thing - a loss for your company. At best, the loss is a matter of productivity. At worst, the loss could be in court. The only thing standing between your company and such losses is a network usage policy.

### **Network Usage Policies: Who Needs Them?**

Network Usage Policies are simply another variation of the policy/procedure theme. Put simply, a Network Usage Policy sets rules and standards by which employees are able to access and use workplace technology. Network Usage Policies range in complexity and ubiquity from one-page memos posted in the employee cafeteria, to detailed, multi-page addenda to the employee handbook and pop-up screens triggered by logon. Network Usage Policy effectiveness pretty much fits along the same continuum.

According to a PC World survey, nearly 58 percent of employers who monitor employees' Internet use do so to crack down on recreational use; 47 percent hope to stop employees from downloading pirated software; and one-third want to speed up Internet connections by eliminating recreational browsing and excessive downloads.[vii] The emerging issue of importance with inappropriate Internet surfing, however, is legal liability.

The best Network Usage Policies include specifics on acceptable uses, rules of online behavior, access privileges and penalties for violations of the policy, including security violations.

#### **Covering All the Bases**

When people think about Network Usage Policies, they often think no further than the Internet and/or intranet access. However, there are many other areas of potential trouble that should be included. For maximum protection, it's wise to include all communications devices - telephones, Email, voice mail and fax machines.

#### **The Perils of Email**

Email can be the source of a host of problems, as recent court cases have shown. The modern-day version of the office water cooler, Email can be an incredible productivity siphon as employees spend inordinate amounts of time writing to friends, family or other non-business recipients. And that's the least of it.

Under the guise of circulating jokes, employees can use it to disseminate racist or sexist material - material for which the company can ultimately be held responsible. A long shot? Consider *Owens v. Morgan Stanley & Co.* In this recent case, African American employees received the green light to proceed with action against the company for discrimination and retaliation arising from alleged isolation and denial of advancement opportunities after they complained about the internal dissemination of an Email message containing racist jokes.[viii]

Employees can also denounce company policy and/or officials using broadcast Emails to several other, if not all, employees -- and evade termination for it. That's precisely what happened in *Timekeeping Systems Inc. v. Leinweber*, which involved an employee who was terminated after he criticized the company's employment policies in an Email message to all employees.[ix] The company terminated the employee, but had to reinstate him after the National Labor Relations Board (NLRB) upheld his right to use internal email to dispute the fairness of a new company vacation policy and challenge the truthfulness of the company CEO's assertions about the policy. The NLRB held that such remarks, though arrogantly expressed, were within the scope of National Labor Relations Act-protected "concerted activity," since they assisted the employees' discussion of and response to the new policy.[x]

#### **The Internet: When Surfing Hurts**

Like Email, the Internet can be a massive time waster. Even seemingly innocent surfing is taking up a lot of time in a lot of companies. Between 19 million and 26 million Americans have Internet access at work.[xi]

On average, each spends approximately six hours each week online. A significant portion of those hours is spent on activities other than work. Take shopping: According to Active Research, Inc., a San Francisco Web-based market research firm, retail clicks crank up at 9 a.m. and spike near lunchtime. [xii] [JSH1] Or gaming: Internet games site, Gamedealer.com, gets most of its orders -- 65 percent -- Monday through Friday, between 9 a.m. and 5 p.m.[xiii]

Online shopping can strain other company resources in addition to productivity. Someone -- namely, the company mailroom -- has to handle all those packages that get ordered. And where there are shoppers, there are cookies, information that a website puts on a surfer's hard disk so it can remember something about that surfer -- such as shopping preferences -- at a later time.[xiv] Cookies lead to spam (the Internet's version of junk mail), which can clog up your network, put a serious drain on bandwidth and response time and trigger expenses for additional equipment to handle all the unnecessary traffic.

Productivity lost to shopping and gaming can cost a company thousands of dollars, but another offshoot of inappropriate Internet surfing at work -- legal liability -- can cost millions. Unfair as it may seem, companies can be held liable for what employees do with company resources. If employees surf to pornography sites while at work, they may be doing more than wasting time -- they may be setting the company up for a sexual harassment lawsuit. How? By creating something known as a "hostile work environment.

"Title VII of the Civil Rights Act of 1964 defines two types of sexual harassment: quid pro quo, in which sexual favors are traded for tangible job benefits; and hostile workplace, which is abusive conduct sufficiently severe and persistent to affect seriously the psychological well-being of the victim.[xv] To prove quid pro quo harassment, victims must typically show tangible job detriment, which is often difficult to do.[xvi] As a result, the litigation focus of claimants has shifted toward the hostile workplace claim, which does not depend on the trade of sex for job benefits[xvii].

**Other potential legal issues arising from employee misuse of Internet access include:**

- Copyright violation from downloading protected information.
- Defamation, if an employee decides to slam the competition online.
- Illegal gambling operation over the Internet.[xviii]

**Minding the PBX and Fax**

Companies that do have Network Usage Policies often limit them to Internet and Email. But by overlooking phones and fax machines, they're overlooking a source of significant expense and potential security breaches. Today's hackers don't limit themselves to cracking the company intranet. Using sophisticated, readily available system tools, hackers can get in via the PBX and wreak all kinds of havoc, from running up long-distance charges, to stealing confidential information.

Like Email, voicemail and fax transmissions can put a company in the legal line of fire if deemed inappropriate, sexist or racist. And if an employee uses the fax machine or a computer fax program to send mass mailings of a promotional nature, your company could run afoul of federal laws that make it illegal "to use any telephone facsimile machine, computer or other device to send an unsolicited advertisement to a telephone facsimile machine." [xix]

Usage policies that prohibit this kind of activity may prevent employees from unwittingly engaging in behaviors that expose the company's network to outside automated hacker attacks.

#### **The Employee Response**

So what are companies doing about the problem? According to a PC World survey of top executives at 200 companies, one in five firms had disciplined employees for improper Internet use - from taking away their surfing privileges to taking away their jobs.[xx] In fact, one-third of the companies surveyed already monitored where their employees went on the Internet, and another 12 percent planned to start within a year.[xxi]

A more recent survey conducted by Computerworld (1999) suggests that more than half of companies have still neglected to write and institute usage policies. The survey of 102 network administrators showed that only 40% had written Internet usage policies that prohibit specific online activities.[xxii]

Not surprisingly, Network Usage Policies get mixed reviews from employees. Undoubtedly, the worst offenders are the people who hate them most. But even occasional offenders or non-offenders can find Network Usage Policies disturbing. What, they say, happened to privacy and a little something called The First Amendment? Don't employees have rights, too?

Most companies - who are at risk for employee behavior - now hold the opinion that employee privacy ends where the company communications infrastructure begins. And, for now, the courts are supporting their position.

Increasingly, courts are sending a clear message that employees really have no right to expect privacy in Email, voicemail and Internet usage. Some recent examples include:

**McLaren v. Microsoft Corp., No. 05-97-00824-CV (Texas Ct. App., May 28, 1999).** Employee's use of a private password to encrypt email messages stored on an office computer did not prevent company from decrypting and viewing files. Email account and workstation to use it were provided for business, not personal, use, and company had legitimate access to data stored there.[xxiii]

**Smyth v. The Pillsbury Co., 914 F. Supp. 97 (E.D.Pa. 1996):** A company employee has no reasonable expectation of privacy in his use of internal Email to communicate with a supervisor, even if the company asserts that Email communications would be kept "confidential." Court upheld company's right to intercept the employee's Email and to terminate him for transmitting "inappropriate and unprofessional" communications over the company email system.[xxiv]

**Bourke v. Nissan Motor Corp., No. B068705 (Cal. Ct. App., 7/26/93):** Employers have a right to monitor employees' Email and to terminate them for sending Emails of a personal, sexual nature. Wiretap and privacy laws did not protect employees from employer monitoring.[xxv]

In most cases, companies can be assured of being well within their rights to monitor or block employees' Internet access, because there are no laws on the books that can be interpreted as prohibiting an employer from watching what its employees do on the Internet.[xxvi]

Understandably, many employees are uncomfortable. In a recent online survey, eMarketer found that 50 percent of respondents strongly agreed that companies should be barred from monitoring employees' Email.[xxvii]

Surprisingly, another survey showed that a greater number of employees - 94.2 percent - felt that monitoring was fine, as long as they knew about it.[xxviii] This response points to a key issue: If you have a Network Usage Policy, it makes good sense to make sure everybody knows about it. In fact, to give it the teeth it needs to hold up in court, it's wise to make sure that every employee signs it.

Federal law does offer employees a minimal degree of protection via The Electronic Communications Privacy Act (ECPA), which generally prevents employers from monitoring personal communications, such as private phone calls, unless there is reason to believe a crime has occurred, or certain other exceptions.[xxix] However, the ECPA also supports an employer's right to monitor stored electronic communications, such as voicemail and Email messages, in order to protect its business, rights or property.[xxx] And employers do have some restrictions in monitoring personal communications - namely, employees must give their consent.[xxxi] If employees anticipate monitoring and clearly understand its purpose, they will most likely accept it as another fact of business life.

#### **A Network Usage Policy Primer**

Network Usage Policies can increase employee productivity and limit the legal liability facing companies. Lawyers like them because they allow companies to be proactive rather than reactive to potential liability - the classic best-defense-is-a-good-offense argument.

But developing a Network Usage Policy can be tricky. What's legal is a moving target right now, a complex combination of both state and federal law, and, in the case of e-commerce, international law.[xxxii] Laws are clear in some jurisdictions; nonexistent in others.[xxxiii] Therefore, companies must develop unique policies based on their specific needs and the laws regarding their industries. That being said, following are just a few points to consider when drafting a Network Usage Policy.[xxxiv]:

#### **General guidelines**

- Does your policy indicate that the company owns and controls all workplace technology and therefore all communications and activity conducted over it?
- Does it tell employees not to expect privacy through company Email, Internet usage, any created documents or voicemail?
- Does it cover telecommuting activities?
- Does it address passwords, including how they are assigned, how they can be changed and shared?

#### **Email**

- Who can use it and for what purpose?
- Are personal messages allowed?
- Who can access employee Email?
- Can they do it without employee consent?
- Does the company monitor Email? If so, how, when and under what circumstances?
- Can employees receive large Email attachments?
- Are specific Email activities (i.e., gambling, copyright infringement, transmitting trade secrets, etc.) expressly forbidden?
- Does the policy prohibit sexist or racist content? How are violations handled?
- Does it limit forwarding of both in-house documents and external messages such as virus hoaxes and chain letters?

#### **Internet Usage**

- When and how can the Internet be used during the workday? What about off-hours surfing?
- Will the company monitor Internet usage? If so, how, when and how often?
- Are specific activities forbidden, such as downloading software or files from the Internet?

These are just the tip of the iceberg. What your company should include in its Network Usage Policy depends on what your company does and what its unique exposure might be. But no matter what type of policy you develop, the key to making it work is enforcement.

#### **Making it Stick**

The best laid Network Usage Policies of mice and men often go astray - especially if they're not enforced.

For starters, your Network Usage Policy should clearly state what violators can expect, from an informal warning all the way to dismissal and criminal prosecution. And, by all means, do what you say. Having an established policy, then enforcing it unevenly or not at all can put your company at risk for litigation.

Make sure employees know what you're doing and make sure they agree to it by formally acknowledging having read it and signed off on it. Then, make sure employees never forget about it. Talk about it in seminars, post it all over the place, have a message pop up when employees log on - employees should never be able to say they "just didn't know." At the very least, an annual reminder of the policy should be sent to all employees.

Finally, make sure you have an effective way to monitor what's really going on. Network usage reporting software can help your company head off problems before they happen and document them accurately if they do.

Like the Network Usage Policy, a company's network usage data will invariably reflect the unique nature of its business, its policies and its employees. What constitutes suspicious activity depends on your network and may be perfectly normal behavior on another company's network. The important thing is for a company to understand how its network should be used - which the Network Usage Policy spells out - and to monitor that usage to detect unusual patterns.[xxxv]  
In short, effective Network Usage Policies follow the four Cs - they are clear, comprehensive, communicated and compelled.

### **Striking the Balance**

One thing is clear: Without an effective communications infrastructure, a company cannot hope to survive. The trick is to optimize the significant benefits of today's communication devices while minimizing their equally significant risks. An effective Network Usage Policy can help your company strike the balance.

[i] <http://www.eeoc.gov/stats/harass.html>

[ii] Ibid.

[iii] Hershey, Robert D., "Some Abandon Water Cooler For Internet Stock Trading,"  
New York Times, May 20, 1999

[iv] Ibid.

[v] Ibid.

[vi] Chartrand, Sabra, "Patents; A new software program takes aim at personal long-distance phone calls made by employees," New York Times, March 22, 1999.

[vii] "The Need for Monitoring," PC World, November 1997,  
<http://www1.pcworld.com/workstyles/online/articles/nov97/1511p245e.html>.

[viii] The Perkins Coie Internet Case Digest,  
<http://www.perkinscoie.com/resource/ecommerce/netcase/Cases-09.htm>.

[ix] Burke, Thomas P., Dolan, Brendan G. and Gleason, Paul M., "Email Workplace Issues,"  
<http://www.brobeck.com/docs/98features/0898.html>.

[x] The Perkins Coie Internet Case Digest,  
<http://www.perkinscoie.com/resource/ecommerce/netcase/Cases-09.htm>.

[xi] Plotnikoff, David, "Firms watching office Web use," Knight Ridder Tribune,  
<http://www.netoutcome.com/html/star.html>.

[xii] De Lisser, Eleena, "One-Click Commerce: What People Do Now to Goof Off at Work,"  
the Wall Street Journal...

[xiii] Ibid.

[xiv] <http://www.whatis.com>.

[xv] Fishman, Steven J., "Sex in the Workplace: Searching for a Clear Path," Michigan Forward,  
August 1998, [http://www.voyager.net/mcofc/publication/michigan\\_forward/9808mf/sex.htm](http://www.voyager.net/mcofc/publication/michigan_forward/9808mf/sex.htm).

- [xvi] Ibid.
- [xvii] Ibid.
- [xviii] "Other legal minefields," PC World, November 1997,  
<http://www1.pcworld.com/workstyles/online/articles/nov97/1511p245f.html>.
- [xix] Jonathan Byrne, Squeezing Spam Off the Net: Federal Regulation of Unsolicited Commercial Email, 2 W. Va. J. L. & Tech. 4 (Feb. 14, 1998), <http://www.wvjolt.wvu.edu/v2i1/byrne.htm>.
- [xx] Martin, James A., "You Are Being Watched," Computer World, November 1997,  
<http://www1.pcworld.com/workstyles/online/articles/nov97/1511p245.html>.
- [xxi] Ibid.
- [xxii] Computerworld, "Internet Usage Policies," March, 1999
- [xxiii] The Perkins Coie Internet Case Digest,  
<http://www.perkinscoie.com/resource/ecom/netcase/Cases-09.htm>.
- [xxiv] Ibid.
- [xxv] Ibid.
- [xxvi] "Is Monitoring Legal," PC World, November 1997,  
<http://www1.pcworld.com/workstyles/online/articles/nov97/1511p245j.html>
- [xxvii] [http://www.emarketer.com/estats/epoll\\_alone.html](http://www.emarketer.com/estats/epoll_alone.html)
- [xxviii] <http://www1.pcworld.com/workstyles/online/articles/nov97/1511p245d.html>
- [xxix] "Is Monitoring Legal," PC World, November 1997,  
<http://www1.pcworld.com/workstyles/online/articles/nov97/1511p245j.html>
- [xxx] Ibid.
- [xxxi] Ibid.
- [xxxii] Shimpock, Kathy, "Guidelines for Developing Business E-Policies," Solutions@Law,  
<http://www.solutionsatlaw.com/it/techarticles/epolicies.htm>.
- [xxxiii] Ibid.
- [xxxiv] Ibid.
- [xxxv] Tadjer, Rivka, "Safeguard Your IT Assets," InternetWeek Online, May 31, 1999,  
<http://www.commweek.com/change/change053199-1.htm>.