



## Internet Usage And Legal Liability

### Limiting Potential Liability

Organizations of all sizes take steps to limit their legal liability while conducting their daily operations. Unfortunately, many of the same businesses that take extraordinary measures to protect themselves in the real world are exposed to costly and damaging liability issues that have their origins in cyberspace. This paper will attempt to explain the nature of these threats and illustrate how a well-coordinated approach to Internet Access Management can help an organization limit its exposure.

### Liability Is Only One Click Away

The Internet is a powerful tool for business, but if its use is not managed correctly, inappropriate, offensive and illegal content can be just one click away. The following examples indicate the scope of the liability problem faced today by organizations of all sizes:

- 27% of Fortune 500 companies have battled sexual harassment claims stemming from employee misuse and abuse of corporate e-mail and Internet systems. *Source: American Management Association*
- More than 60% of companies have disciplined employees – and more than 30% have terminated employees – for inappropriate use of the Internet. *Source: The Center for Internet Studies*
- Dow Chemical Co. fired 50 employees and disciplined 200 others after an e-mail investigation turned up hard-core pornography and violent subject matter. *Source: Associated Press*
- 70% of employees admit to viewing or sending adult-oriented personal e-mail at work. *Source: NFO Worldwide*

### All Organizations Are At Risk

If an organization has even one employee accessing inappropriate or illegal content, it puts the entire organization at risk. A few examples of how an organization can be held liable for the Internet activity of an employee:

- **Sexual Harassment** – An employee viewing pornography at his workstation puts the organization at risk if another employee sees something offensive and files a grievance or lawsuit against the organization.
- **Illegal Activity** – organizations can be held responsible if an employee accesses or disseminates illegal information, or uses that information to commit a crime.
- **Child Pornography** – some states are passing laws or considering legislation that would require IS personnel to report any evidence of child pornography to authorities.

- **Discrimination** – An employee using the Internet to access content that espouses hate or discrimination puts the organization at risk. If that individual is in a position of authority or responsible for hiring decisions, civil rights investigations could result.

In a recent study commissioned by N2H2, Incorporated, IS decision-makers rated liability as the most important and urgent Internet management concern. Interestingly, those same IS professionals reported pressure to solve liability problems comes overwhelmingly from their organization's senior management. So while implementing a solution may be the responsibility, of the IS department, the pressure to apply that solution often originates with senior management outside of the IS department.

### **The Costs Of Liability**

The costs associated with defending an organization against claims of harassment, disciplining or dismissing employees who abuse Web access, and repairing a company's reputation can be staggering. What follows is by no means an exhaustive list of potential costs, but is presented to illustrate the scope of the potential problem.

- **Litigation And Settlement Costs**

According to one prominent Seattle Law Firm, the average cost to litigate a hostile-workplace or sexual harassment claim is \$250,000. And the average cost to settle a claim is almost 10 times that amount! In a recent case where a dozen employees were subjected to a hostile work environment through their exposure to sexually explicit material on unrestricted computer screens, the EEOC ruled that the Minneapolis Public Library could be liable for more than \$1 million in settlement fees. Clearly, the benefits of a solution that minimizes exposure to this kind of liability far outweigh the costs.

- **The Cost Of Terminating Employees**

Defending an organization against litigation is a waste of precious resources. But what about dealing with employees who access inappropriate content on the job? Just catching a person in the act or proving they did something wrong is only the first step in what, for many organizations, can be a long and painful process. Legal fees associated with dismissing employees can be substantial, especially if there's a union or other employee advocate involved. Additionally, the lost intellectual knowledge and training investment in that employee is a very real cost that cannot be re-captured. Once those costs have been absorbed, the organization must still foot the bill for hiring and training a replacement.

- **The Impact On Good Employees**

Not all employees affected by inappropriate content in the workplace take action. Some individuals who are exposed to inappropriate Internet usage simply lose respect for the person causing the problem. If nothing is done to address the issue, they may even lose respect for the company. Teams start to become dysfunctional and productivity slips. Eventually, the affected people quit – often without even telling the HR staff the reasons why. This silence can be costly for an organization, with estimates indicating that as many as ten people quit for every one that takes aggressive action.

- **Costs To An Organization's Image Can Be Incalculable**

Perhaps what's most difficult to measure is the price of a damaged reputation resulting from the publicity of protracted legal action. Companies spend literally billions of dollars nurturing and developing their brands. All of that investment can be undone in a matter of days by the public relations nightmare of a high-visibility lawsuit. But this problem does not just affect the private sector. The risk to government organizations can be even greater. Since all Internet log-files are a matter of public record, any agency's Internet usage is open to public inspection. One employee accused of accessing inappropriate content while using taxpayer-owned resources can become a political firestorm.

### **Protecting An Organization**

Fortunately, organizations have many tools to protect themselves against possible legal liability stemming from Internet use. Acceptable Use Policies, education and training, and the proper Internet management technology are all useful in limiting an organization's exposure. Ideally, a combination of methods gives an organization the best chances for managing Internet usage and protecting against the possibility of legal liability.

### **An Internet Use Policy Is Only The First Step**

In N2H2's recent survey of IS decision-makers, over 75% of those whose organizations provided Internet access indicated that they have some sort of acceptable use policy in place. Acceptable Use Policies can take many forms, but all are fundamentally a tool used by organizations to outline what constitutes appropriate Internet use.

Since each organization has its own unique culture, it's important that an Acceptable Use Policy be tailored to the specific needs of the people who use the Internet to do their jobs. There is no "one size fits all" solution. A traditional banking or insurance firm might have a tightly controlled vision of what constitutes appropriate workplace Internet use, while a high-technology firm may have a somewhat less restrictive view. But both organizations will probably agree that content promoting hate, pornography or illegal activity has no place in the workplace and that it's this kind of



content that leads to most of the legal liability issues associated with Internet use.

### **Training And Education**

Once an Acceptable Use Policy has been formulated, it's important for the organization to educate and train employees to ensure that the fundamental principles of the policy are instilled throughout the organization. Simply presenting the policy as another set of regulations will tend to make most employees ignore the message completely. Successful organizations not only tailor their policies to reflect their culture; they encourage discussion and feedback in order to promote buy-in and ownership. Keep in mind, it costs the same to dismiss an employee who didn't read or completely understand a policy as it does to fire an employee who willingly broke the rules. It's much more cost-effective to educate the entire organization before a problem occurs.

### **Conclusion**

Organizations require solutions that enable users to access the information they need while limiting the organization's exposure to legal liability or a public relations nightmare. A robust and versatile Internet filtering product can help an organization implement a policy-based Internet use management solution that limits exposure to potentially costly and devastating legal liability issues. Services and solutions that help you understand Internet usage and tools that enable you to protect your organization from Internet abuse are available from reputable software vendors such as N2H2.

With core expertise in categorizing Internet content and developing products that help deliver only content that's appropriate for an organization's needs, N2H2 is providing important tools in the arsenal to help protect organizations from the legal liability issues that arise from Internet usage in the workplace.

### **For More Information**

To find out more about N2H2's versatile filtering products and the advantages of managing your organization's Internet access and activity, contact N2H2 today at **800 971 2622** or visit them on the Web at <http://www.n2h2.com>