MessageLabs®

Be certain

Legal Risks of Uncontrolled Email and Web Content

Hillel I. Parness
Professor, Columbia Law School
Of Counsel, Lovells (New York)

Table of Contents

The starting point is that employers will generally be held responsible for the acts of their employees; the principle of vicarious liability.

Introduction

Email is critical to many businesses; its ease of use, combined with the speed and scale of distribution, make it an invaluable business tool. Today, many businesses could not function without consistent and unfettered access to the Internet. However, these same attributes can also cause severe difficulties for employers if employees' use of email and the Internet is not controlled adequately. This short summary considers some of the risks that employers face. It is not a comprehensive study of the topic; therefore, detailed legal advice should always be sought in specific situations.

THE RISKS

The starting point is that employers will generally be held responsible for the acts of their employees; the principle of vicarious liability. An employer is vicariously liable for the wrongful acts committed by employees in the course of their employment, and this principle may cover acts of the employee that are incidental to their employment. The potentially wide scope of this is highlighted by the case Riviello v. Waldron, in which the court considered the liabilities arising from an incident in which a tavern employee injured a customer's eye with a knife while demonstrating self-defense. The New York Court of Appeals concluded that the employee's behavior was within the scope of his employment, and that the customer could recover against the tavern owner.

Employers can also be held liable for the actions of their employees on theories of negligent hiring or negligent retention -- if an employer knows or should know of its employee's inappropriate behavior and thereafter allows it to continue. In 2004, the Supreme Court of Iowa allowed a former deputy sheriff to proceed with claims against the county and sheriff for negligent hiring, supervision and retention of another officer. In Kiesau v. Bantz, the plaintiff claimed that another officer had digitally altered a photograph of her to make it appear as if she were topless, and circulated the altered photograph via email.

Aside from the obvious risk that an employee who spends significant periods of the day engaged in personal email correspondence may have a reduced level of productivity and drain IT resources, there are other, more subtle, risks. We consider some of them below.

…the court cited a single piece of evidence – that the supervisor had emailed two sexually explicit short stories to the plaintiff.

Inappropriate material can be distributed by attachments to emails, and this may lead to claims that the employer has failed to provide a "safe" working environment and/or that the conduct of the employees concerned amounts to discrimination. Such activity may also cause the employee affected to resign and claim unfair "constructive" dismissal. Damages awards in discrimination claims are potentially unlimited.

In 1995, Chevron was forced to pay $2.2 million to four female employees– the women had sued for sexual harassment after male co-workers circulated offensive e-mails, including one message that listed "25 reasons why beer is better than women." Similarly, in 1997, a federal judge allowed a harassment case to proceed against Morgan Stanley that was based on allegations that certain employees had distributed a racist email, and then retaliated against black employees that complained about it. Although the judge later dismissed the Morgan Stanley case, these two early examples demonstrate that use of email can create harassment liability for employers.

In the recent case of Lytel v. Simpson, a federal court in California considered claims of sexual harassment based on a course of conduct that included sending inappropriate emails to an employee, and sending emails to her personal email account without permission. The court found the supervisor's behavior so severe that it granted partial summary judgment, a finding of liability without a trial. In support of this ruling, the court cited a single piece of evidence – that the supervisor had emailed two sexually explicit short stories to the plaintiff. As explained in the previous section, this type of liability can extend to employers, depending on the particular facts of the case.

…the court found that the employer could have monitored the employee's computer activity.

CHILD PORNOGRAPHY

It is both a federal and state crime to possess or view child pornography. An appellate court in New Jersey recently allowed a case to proceed against an employer for failing to stop an employee from accessing pornography and sending nude photographs of his daughter to a child pornography site. In the case of Doe v. XYC Corp*, the court found that the employer could have monitored the employee's computer activity, had the right to monitor the employee's computer activity, and had been on notice that the employee had been using his computer to view pornography and child pornography.

DEFAMATION

Defamation cases -- publication of false statements about an individual to third parties – can lead to expensive claims for employers. In the Kiesau case mentioned above, the plaintiff – a former deputy – obtained a jury verdict, and $156,000 in damages, against a fellow officer for circulating an altered photograph of her, on theories of defamation and invasion of privacy. Communications technologies have the potential of vastly broadening the scope of claims in the Internet age. Distribution of defamatory statements by email or through Web sites can exponentially expand the impact of the defamation and thus potentially the damages.

The federal Communications Decency Act of 1996 includes a "good samaritan" provision that shields those who republish third-party content without alteration from defamation and other types of speech-based claims. Since its enaction, this provision has been utilized in a wide variety of cases to immunize "interactive computer services" from liability. Perhaps most famously, eBay, Inc. successfully argued that it was not liable for its users' sales of counterfeit musical recordings because the listings advertising the recordings were created by users without any involvement from eBay (Stoner v. eBay, Inc.). This immunity, however, only applies if the "interactive computer service" is not also the "information content provider" – when a company begins to get involved with the creation of content, or even the editing of third-party content, it runs the risk of losing this protection. In the recent case of Whitney Information Network, Inc. v. Xcentric Ventures, LLC, the 11th Circuit Court of Appeals threw out dismissal of a case because an open question remained as to the authorship of the allegedly defamatory statements, and sent the case back to the trial court for further proceedings.

* note the names of this case are confidential

… many U.S. courts have specifically come to recognize the role that email can play in contract formation.

THIRD PARTY INTELLECTUAL PROPERTY RIGHTS ("IPR") INFRINGEMENT

Information on the web, created by others, is frequently attached to email communication, and this may be in breach of the author's terms. Copyright protected material can be widely circulated by employees who are adept at "cutting and pasting." Employers may then face breach of copyright actions, resulting in expensive litigation and damaging publicity.

The federal Digital Millennium Copyright Act of 1998 updated certain portions of the Copyright Act to deal with the Internet and other digital technologies. The DMCA sets forth certain safe harbors from copyright liability for certain types of parties that operate on the Internet, but only if those parties have commensurate policies and procedures in place that are also spelled out in the DMCA.

Companies must also be cautious when implementing new Internet-based business models that have never been tested in courts of law. In 2000, MP3.com learned this lesson the hard way, when a federal district judge determined that its “Beam-It” service, which was designed to give Internet users access to MP3 versions of music they already owned on compact disc, violated copyright law, and handed down a $53 million judgment against MP3.com (UMG Recordings, Inc. v. MP3.com, Inc.).

CONTRACT FORMATION

Employers are often under the misapprehension that, for a contract to be legally binding, many formal requirements or procedures need to be met or followed. In fact, U.S. courts recognize generally that contracts can be formed under a wide range of circumstances, and many U.S. courts have specifically come to recognize the role that email can play in contract formation.

In In re National Century Financial Enterprises, Inc., a federal court in Ohio recognized that email communications satisfy the contract requirements of signatures and writing, and that weekly emails and reconciliation reports sent from one party to another modified key terms of the sale agreement between the parties, and the parties were bound by the modifications.

A further problem can be that the "disposable" quality of email frequently means that important documents may be destroyed, making it hard to establish exactly what the terms of any contract were in the event of a dispute.

… It is crucial that an employer develops and distributes an Acceptable Use Policy ("AUP"), so that all workers are aware of the employer's policies toward the use of computers, email and the Internet.

CONFIDENTIALITY

Email can be used as a tool to send confidential data outside of the organization, particularly in the case of a disgruntled employee, or one who intends to leave to set up a competing business. This can be highly damaging to an employer, as it may lose sensitive and commercially important information. Aside from the commercial impact, there is also the risk of potential breach of contract or a privacy claim in the event that the information refers to a third party. Privacy claims can arise in many contexts, including the developing group of state and federal privacy statutes.

DEALING WITH THE RISKS

Generally speaking, under US law, companies can monitor employees' computer usage with impunity, because workplace computers and their data are the property of the employers, and also because employees do not have a reasonable expectation of privacy in the workplace. The federal Electronic Communications Privacy Act of 1986, which was amended in 2001, is viewed as codifying the idea that workplace electronic communications in the workplace can be intercepted and reviewed by employers.

Thus, the employer in most circumstances can review employees' email, computer usage and Internet usage when investigating various workplace incidents (although consultation with counsel in such situations is strongly recommended). Monitoring, of course, has its limitations – no employer can monitor everything its employees do at all times, especially when it comes to email and Internet usage. It is therefore crucial that an employer develops and distributes an Acceptable Use Policy ("AUP"), so that all workers are aware of the employer's policies toward the use of computers, email and the Internet.

Additionally, the employer should consider what risks it is trying to avoid, and assess what impact any monitoring may have on its employees. The employer should adopt the least intrusive method of monitoring possible to achieve its legitimate aims. For example, if the problem is excessive use of email by staff, slowing the employer's email system, monitoring of the level of email traffic by individual users, rather than monitoring of the content of such emails, may be sufficient to address the issue.

Clear communication to employees and the protection of a good AUP is vital to reducing the risk of claims by employees. In Bourke v. Nissan Motor Corporation, the California Court of Appeal affirmed the dismissal of invasion of privacy claims against Nissan because the plaintiff employees had signed Nissan's use policy, and therefore could not fault Nissan for accessing their emails.

In developing a monitoring policy, however, one must be careful not to go too far. Recently, for example, the disclosure of monitoring within Hewlett-Packard resulted in criminal charges of five people, including its former chairwoman. It is prudent to not only have legal justification for one's monitoring, but to also assure one's self that whatever steps are taken are proportionate to the risk being addressed. Automated monitoring can be a cost-saving approach, but one should always bear in mind that the ultimate responsibility for ensuring compliance and balanced monitoring rests with the employer, not the supplier of any technical solution.

Summary

All employers should have a clear AUP and ensure that it is enforced consistently. The AUP should explain the risks, indicate what monitoring is to be conducted and why, offer alternatives to employees if they do not wish to use email communication and set out penalties for any breach of the AUP, linking this to the employer's disciplinary policy. The AUP can be supported by appropriate technical solutions, but the employer must ensure that the level of monitoring is proportionate to the risks involved.

www.messagelabs.com
info@messagelabs.com

Call 866-460-0000 for more information

Europe
HEADQUARTERS
1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom

T +44 (0) 1452 627 627
F +44 (0) 1452 627 628

LONDON
3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom

T +44 (0) 207 291 1960
F +44 (0) 207 291 1937

NETHERLANDS
Teleport Towers
Kingsfordweg 151
1043 GR
Amsterdam
Netherlands

T +31 (0) 20 491 9600
F +31 (0) 20 491 7354

BELGIUM / LUXEMBOURG
Cullinganlaan 1B
B-1831 Diegem
Belgium

T +32 (0) 2 403 12 61
F +32 (0) 2 403 12 12

DACH
Feringastraße 9
85774 Unterföhring
Munich
Germany

T +49 (0) 89 189 43 990
F +49 (0) 89 189 43 999

Americas
AMERICAS HEADQUARTERS
512 Seventh Avenue
6th Floor
New York, NY 10018
USA

T +1 646 519 8100
F +1 646 452 6570

CENTRAL REGION
7760 France Avenue South
Suite 1100
Bloomington, MN 55435
USA

T +1 952 886 7541
F +1 952 886 7498

Asia Pacific
HONG KONG
1601
Tower II
89 Queensway
Admiralty
Hong Kong

T +852 2111 3650
F +852 2111 9061

AUSTRALIA
Level 6
107 Mount Street,
North Sydney
NSW 2060
Australia

T +61 2 8208 7100
F +61 2 9954 9500

SINGAPORE
Level 14
Prudential Tower
30 Cecil Street
Singapore 049712

T +65 62 32 2855
F +65 6232 2300