Content Security: The New Legal Risk For Your Business

A Lawyer's guide to the legal implications of Electronic Mail

KEY POINTS

1. **The contents of E-Mail can generate legal action.**
2. **The legal action can be taken against the employer of the person sending E-mail.**
3. **The *best way* to reduce these risks is by implementing a properly written E-mail policy.**
4. ***There is software that can* help: MIME*sweeper* from Content Technologies Inc.**

How E-Mail generates legal actions

Several cases have already found that E-Mail is actionable.

E-Mail has already generated cases involving

- Defamation
- Spoliation of evidence
- Breach of contract
- Sexual Harassment
- Misrepresentation
- Intellectual property theft

Claims have been made by

- Employees
- Employers
- Third parties

Claims by employees

Employees can take action against their employers for:

- **Breach of privacy.** Employers may not have the right to investigate employee's E-mail without authorization. Many States recognise a common law right of privacy and The *Electronic Communications Privacy Act*[1] prohibits the unauthorized interception of electronic communications (including E-mail).

[1] 18 U.S.C. §§ 2510-2710, 18 U.S.C. § 2511(1)(a).

- **Sexual or racial harassment or discrimination** if jokes of a sexual or racial nature are distributed by E-mail internally. Title VII of the *Civil Rights Act* of 1964 prohibits any discrimination by an employer on the basis of gender or race. Interpretations of the act apply further to create the right of an employee to "work in an environment free from discriminatory intimidation, ridicule and insult[2], an especially important point in an environment where racial or sexual material is distributed by internal E-mail.
- **Prevention of Labor organization activities.** Under one interpretation of the *National Labor Relations Act,* if an employer grants permission for personal messages to be distributed by E-mail, employees may also use the system for Labor organization activities. [3]

Claims by third parties against corporations

Legal action can be taken against corporations on the basis of E-mail sent by employees for several reasons, including:

- **Vicarious liability for copyright breach.** An employer may be responsible for copyright breaches committed by an employee if it derived financial benefit from the breach, *even if unaware of the breach*.
- **Contributory liability arising from copyright breach.** Contributory liability may be construed as the employer assisted the employee to breach copyright by providing the E-mail system used to perform the breach.
- **Defamation.** Defamation law applies unconditionally to E-mail. Employers may be found liable for defamatory E-mail if it is found an employee is acting as an agent of the employer, or as a disseminator of defamatory material.
- **Spamming and Spoofing.** Emerging Federal and State Law may impose fines and other penalties on corporations sending large volumes of unsolicited E-mail ("spamming"), especially in cases where the sender of the mail disguises their return addresses and identities ("spoofing").[4]

Distribution of Trade Secrets and other risks

The use of E-mail must also be considered carefully for the following reasons

---

[2] *Meritor Savings Bank v. Vinson*, 477 U.S. 57 (1986).

[3] *See, e.g., Roadway Express, Inc. v. NLRB*, 831 F.2d 1285, 1290 (6th Cir. 1987) (employer may not discriminate against union or other organizing material when it has chosen to allow personal messages on a company bulletin board); Central Vermont Hospital, 288 N.L.R.B. 684 (1988).

[4] Senate Bill 771, introduced by Frank Murkowski (R-Alaska), Cal. Bus. & Prof. Code § 17538.

- **Distribution of Trade Secrets.** The informal nature of E-mail means it is simple for employees of a corporation to distribute documents containing trade secrets. The distribution and reception of such documents must be considered as part of the legal implications of E-mail.
- **Duty to preserve E-mail in pending litigation.** E-mail is admissible in evidence. Deliberate attempts to erase E-mail[5] or inadequate archiving procedures may result in a claim for spoliation of evidence.
- **Discovery of E-mail prior to litigation.** Archived internal E-mail has become a common target during the discovery process.
- **Forgery.** The insecure nature of E-mail means forgery is not a complex process.

How to reduce the risks

To reduce the risk of legal action resulting from E-mail, two steps must be taken

1. Creation of a written E-Mail policy
2. Implementation of software to enforce the policy

Written E-mail policies

A properly written E-mail policy can help to minimize liability for the actions of employees.

E-mail policies should include at least the following elements

1. An explicit statement that **the computer and E-mail system belong to the business,** that employees may use the computer only for authorized purposes.
2. An explicit statement that **employees can expect no privacy.**
3. An explicit statement that the employer has the right, not the duty, to monitor, to impart to the employee the notion that any mail may be read, at any time.
4. A warning to exercise care in drafting E-mail, as E-mail reflects on the business. Moreover, E-mail is easily copied and increasingly the subject of litigation.
5. Explanations of content intolerable to the business.
6. The requirement to sign the policy as acknowledgment it is understood by the employee, and that the employee understands disciplinary action — including termination — may flow from breaches.

MIME*sweeper*: the Content Security software you need to enforce an E-mail policy

MIME*sweeper* enforces an E-mail policy by investigating the contents of every E-mail sent by a corporation, to internal and external destinations.

---

[5] *Shaw v. Hughes Aircraft Co.* (Los Angeles Sup. Ct.), see *Somebody Destroyed the Evidence*, Corporate Legal Times, Vol. 7, No. 70 (Sept. 1997).

How MIME*sweeper works*

To prevent inappropriate content being sent by E-mail, MIME*sweeper* uses a technique called lexical scanning to 'read' every E-mail.

Your E-mail administrator can set the lexical scanner so it assigns points to certain words and sets a points threshold at which an outgoing E-mail will be blocked. Blocked E-mail can be quarantined, for later investigation.

To prevent trade secrets being distributed by E-mail MIME*sweeper* uses lexical scanning to ensure the contents of the E-mail message are not confidential — again using rules set by the E-mail administrator.

To track all E-mail MIME*sweeper* can automatically archive all E-mail, again using rules and lexical scanning if desired to read and archive only selected mail.

To add disclaimers to potentially sensitive E-mail, MIME*sweeper* uses lexical scanning to read the mail and automatically add a disclaimer before the mail is sent. The software can also be set to add disclaimers to individual E-mail addresses, or to an entire mail domain.

To stop offensive or sensitive file attachments, MIME*sweeper* uses another technique called Recursive Analysis. No matter how many times a file has been compressed or altered, Recursive Analysis breaks down the file to its constituent components so lexical scanning can be performed.

To stop junk E-mail MIME*sweeper* can be set to automatically reject mail from certain sources.

MIMEsweeper and your existing software and hardware

MIME*sweeper* runs on Windows NT 4.0 or better and requires a Pentium server with 64M of RAM and 500M of hard disk space.

MIME*sweeper* works with all SMTP compliant mail products, and is also available in versions tailored to:

- Microsoft Exchange
- Lotus Domino

MIME*sweeper* works alongside many anti-virus products, which can be integrated with MIME*sweeper* to extend content security to virus protection.

MIMEsweeper and the Web

All of MIME*sweeper's* functions can also be applied to incoming traffic from the World Wide Web.

DISCLAIMER

This Guide is intended to provide general information only, and should not be construed as legal advice or opinions on specific facts or your specific requirements, and Content Technologies will have no responsibility or liability with respect to your use of any of the information provided. Please contact Content Technologies on 1-888-888-6883 if you would like any specific advice.

About this guide

This guide is based on

"Computers, E-mail, And The Internet: Policies, Guidelines, Responsibilities And Risks"

By Michael R. Overly

Michael R. Overly is special counsel to the Information Technology Department at the law firm of Foley & Lardner in Los Angeles, California. He counsels clients on software licensing, copyright, electronic commerce, and Internet and multimedia law. Mr. Overly writes and speaks frequently on these subjects. Prior to becoming an attorney, Mr. Overly worked as a research engineer in the Space and Technology Division of TRW Inc., Redondo Beach, California. He received his MSEE and BSEE from Texas A&M University, College Station, Texas, and his JD from Loyola Law School in Los Angeles.

The book contains an extensive selection of clauses suitable for inclusion in E-mail policies. If you have any comments or suggestions concerning this book, please send them to moverly@concentric.net