



THE JOURNAL OF
**DIGITAL FORENSICS,
SECURITY AND LAW**

**Journal of Digital Forensics,
Security and Law**

Volume 8 | Number 3

Article 1

2013

Risk Management of Email and Internet Use in the Workplace


John Ruhnka

University of Colorado, Denver

Windham E. Loopesko

University of Colorado, Denver

Follow this and additional works at: <https://commons.erau.edu/jdfsl>

 Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

Recommended Citation

Ruhnka, John and Loopesko, Windham E. (2013) "Risk Management of Email and Internet Use in the Workplace," *Journal of Digital Forensics, Security and Law*. Vol. 8 : No. 3 , Article 1.

DOI: <https://doi.org/10.15394/jdfsl.2013.1148>

Available at: <https://commons.erau.edu/jdfsl/vol8/iss3/1>

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.



(c)ADFSL



RISK MANAGEMENT OF EMAIL AND INTERNET USE IN THE WORKPLACE

John Ruhnka
University of Colorado Denver
Phone: 720-375-2992
Fax: 303-315-8084
john.ruhnka@ucdenver.edu

Windham E. Loopesko
University of Colorado Denver
Phone: 720-212-0780
Fax: 612-917-0780
windham.loopesko@ucdenver.edu

ABSTRACT

The article surveys the changing risk environment for corporations from their employees' electronic communications. It identifies the types of liabilities that corporations can incur from such employee communications. It discusses the objectives of corporate internet use policies and the types of provisions such policies should contain. It suggests an alternative risk-based approach to corporate acceptable use policies instead of a traditional "laundry list" of internet use prohibitions.

Keywords: email acceptable use policies, internet risk management, corporate networks, liability for corporate communications, duty to retain emails, liability for employee acts

1. INTRODUCTION

This article presents an overview of some of the potential legal exposures a company can face from employee use of email and internet in the workplace and discusses various approaches to managing and limiting these risks. Electronic communications is the nerve center for today's business. Virtually every business above sole proprietor size (and even many of them) relies on the internet and email for both internal and external communications including marketing, transactions with prospects, customers and suppliers; employee access for operations record-keeping; and often other electronically stored information tools including remote network access and data interchange, cloud computing and social media.

The volume of electronic business communication continues to grow exponentially. In 2011, estimates show 788 million corporate email accounts

(corporate emails representing some 25% of total emails), a number forecast to reach 1.07 billion in 2015 (Radicati and Hoang, 2013). The total number of emails sent globally in 2010 was 1.07 trillion (Yarow, 2013). The Radicati Group Email Statistics Report 2011-2015 indicates that the average corporate user exchanged 105 emails per day (sending only half as many as they received, an estimated 19% being spam, despite spam filters). Daily emails per corporate user are expected to hit 125 by 2015 (Pingdom, 2013). Instant messaging (IM) and social networking growth is even more rapid. IM accounts, estimated at 2.6 billion worldwide in 2011, are forecast to reach 3.8 billion by year-end 2015 (11% annual growth), while the number of social networking accounts (2.4 billion in 2011) is expected to grow to 3.9 billion during this time.

Not all employee time spent accessing workplace networks is necessarily beneficial to the enterprise. One estimate is that slightly over one-third of office time is spent on non-productive activities (PBT Consulting, 2013), such as personal emailing, web surfing, using social media personally, or even watching pornography—and that 25% or more of employees engage in this last activity at work (Mailguard, 2013). There are also significant potential costs associated with business email and internet use beyond wasted employee time or productivity loss. The direct costs of confidential data breaches can range from significant to catastrophic—not counting the “knock-on” effects of reputational harm and lost customers; the Ponemon Institute estimate the costs for US companies at \$188 per compromised record and \$5.4 million per incident. Employees can expose businesses to significant legal claims through using the internet, corporate emails and other electronic communication tools. A corporation’s legal responsibility for employee communications if committed “within the scope of employment” is a very broad concept and is well established. Further, corporate liability for harm embodied in or triggered by employee electronic communications can exist even if such actions were inadvertent or unauthorized. Few if any legal “safe havens” or effective defenses exist that corporate information officers (CIOs) can use to shield their companies from legal liability for employee email misuse or intentional abuse, even if the liability-creating communication was specifically prohibited.

2. MANAGING CORPORATE COMMUNICATIONS IN A CHANGING ENVIRONMENT

The task of risk management and protecting corporate networks, communications and data has been made increasingly difficult due to increased remote accessibility of corporate internal and external networks. Workplace expectations, particularly among younger “millennial” workers, are evolving. The Cisco 2011 Annual Security Report provides the following statistics:

- 81% of college students reported that they should be able to choose their own devices to do their jobs, and 71% believe that company-issued devices should be available for both work and free time, because the boundary between the two is disappearing.
- 56% of college students said that, if a prospective employer bans social media access, they would either decline the company's job offer or, if they accept it, would find ways to access social media in the corporate setting despite the policy.
- 64% of students say they plan to ask prospective employers about social media policies, and 24% said that social media policies would be a key factor in their job decision.

These new attitudes—likely to become more widespread in the working population—are obsoleting older strategies of making a company's IT network an impregnable fortress. A “bring your own device” culture means that a corporation's security perimeters are less subject to centralized control. With more employee work done off-site, and increasing adoption of productivity-enhancing tools such as mobile device communications, remote corporate network access and cloud computing, plus greater use of social media, companies are investigating more proactive approaches to limit potential legal exposure from employee corporate communication activities that focus on risk management of specific corporate activities with high potential legal exposures.

CIOs, human resource directors and legal advisors responsible for developing corporate email and internet risk management policies have a difficult job. They need to protect the company's intellectual property, confidential information and business activities from inadvertent or harmful interference, disclosure or misuse by rogue employees, or outsider access—and they must also develop internet and email risk management policies that will not unduly interfere with employees' effective use of emerging communications technologies and will support a workplace environment where employee talents can flourish. Two key objectives in designing corporate internet and email use policies are that they should be “appropriate” and at the same time “reasonable”, but exactly what do these words mean in this context? Keystroke monitoring and other technologies enabling continuous and intrusive surveillance of employee email and internet use are widely available, and many companies impose outright prohibitions on workplace use personal devices and social media. However, most employees are hardworking and dedicated, and CIOs and others in their zeal to protect the corporation must not create an oppressive or fear-inducing workplace environment. The goal of internet and email risk management policies is to assure a reasonable degree of risk limitation without being unnecessarily intrusive or objectionable. To do so,

these policies need to be based upon an accurate, up-to-date understanding of the legal and economic risks of email or internet misuse *applicable to the specific company's operations*, and in this light to impose employee use rules and restrictions which reduce potential identified risks at the earliest possible stage while not being too costly in terms of employee acceptance, efficiency or morale.

3. LEGAL LIABILITIES THAT CAN RESULT FROM BUSINESS EMAIL AND INTERNET USE

The attorney authors have conducted extensive research about specific legal liabilities that can result from internet and electronic communication activities in the workplace. The following list of legal issues associated with business email or internet use in the workplace has been derived from a review of relevant federal and state court cases, academic articles on the subject and curricula on potential business legal exposures presented by law firms and other service providers who are active in this area (Mailguard, 2013).

3.1 Types of Legal Liability

3.1.1 Entry into Unintended Contracts

Third persons entering into agreements with employees who appear to have standing to enter into a commercial arrangement on behalf of a company are protected against later company claims that the contract is unenforceable because the employee or agent was not unauthorized—by an agency law provision called “apparent authority”. This doctrine holds that a corporation is liable for an employee’s promises to a third party even if the agent had no actual authority for such promises—if the employee or agent reasonably “appeared” to have such authority. The rationale is that a corporation is legally responsible for designating which employees and agents do and do not have the authority to enter into binding contracts on the company’s behalf, including preventing situations where a third party might reasonably believe an employee without specific transactional authority was so authorized.

Another closely related doctrine that often arises in wrongful discharge lawsuits is called “implied contract”. This doctrine holds that workplace “promises” to employees that can reasonably be implied from oral and written statements and job-related actions by corporate managers about future positions, wages, job performance, etc., can be asserted by the employee against the company in wrongful discharge lawsuits. Thus, a manager cannot promise an employee a future raise and then soon thereafter fire him/her for sub-par performance, since the promise of a raise implied that present performance was satisfactory or better.

3.1.2 Negligent Misstatements

This legal doctrine is intended to protect third parties who have been told and have relied upon a “material fact” (important and binding) about a product, service, purchase or hiring decision of a company by an employee or agent. Negligent misstatements can include representations that a product has a specific warranty or can be returned within 30 days of purchase, or that a company will pay a new employee’s moving expenses. While such misstatements are usually oral, they can also occur in or be subsequently referenced in emails, sales presentations and other client communications. Similar concerns arise in law, accounting and investment advisory firms where special legal responsibilities attach to all corporate communications that could reasonably be considered by clients or third parties to constitute legal, tax or investment advice.

3.1.3 Sexual/Workplace Harassment/Pornography

Sexual harassment claims unfortunately can occur in almost every business and can be very damaging to a company, both financially in litigation expenses and damages as well as in terms of employee morale and public image. “Inappropriate sexual attention” in the workplace can occur in various ways, including offensive emails or instant messaging, or the display (even if inadvertent) or transmission of sexually offensive materials or links from the internet.

3.1.4 Gender and Age Discrimination

Gender and age discrimination lawsuits in the workplace are almost always supported by incriminating corporate emails either to or about the wronged employee that support the employee’s later claims of prohibited discriminatory actions.

3.1.5 Defamation

Defamation involves unauthorized public disclosure of embarrassing or damaging unproven accusations (such as workplace sexual harassment, theft or drug use) as well as disclosure of personal information (even if true) which an employee or client has a reasonable expectation will remain private—such as drug test results, medical records or even performance evaluations or salary information—to any third party who doesn’t have a “need to know” the information for legitimate internal management purposes.

3.1.6 Duties of Confidentiality

For many corporations, today’s most valuable assets are often intangibles—such as patents, brands, trademarks, copyrights and customer lists. At least some intangibles involve trade secrets or proprietary know-how and need to be kept confidential to preserve their value, especially if licensed to others or from

others. Other critical internal strategic information such as future product development plans, marketing plans, R&D projects and results, merger and acquisition discussions and company internal financial results prior to SEC reporting and disclosure, need to be kept confidential to protect the company's interests and to avoid potential legal liabilities—such as insider trading charges—resulting from improper disclosure or use.

3.1.7 Employee Expectations of Privacy

Employee privacy is another rapidly evolving area of the law, and the extent of privacy rights can vary considerably among states. Generally, employers may monitor employee communications in the workplace, even if private, if they announce in advance their intent to do so and follow their announced procedures. Companies must, however, establish and follow announced privacy policies to avoid liability for privacy violations.

3.1.8 Virus Transmission

Potential legal liability exists if files contaminated with a harmful virus are carelessly transmitted to others without prior warnings.

3.2 The Duty to Retain Electronic Communications Potentially Relevant to Litigation

Companies also have a duty to retain electronic communications that might create liability. Prior to the landmark federal decision in *Zubulake v. UBS Warburg* (2003) on the corporate duty to preserve potentially incriminating internal emails, many corporations were using electronic records management programs that attempted to limit liability from potentially incriminating internal emails by destroying email server back-up tapes at frequent intervals. However, the *Zubulake* court ruled that once a party *reasonably anticipates litigation could result from its activities* (no actual litigation need yet be filed), a “litigation hold” attaches to all electronic records, and it must suspend any routine electronic record destruction policies and preserve all potentially relevant records. Thus, today it is common practice for corporate internal emails to be preserved indefinitely for the eventuality of litigation or governmental investigations. Different or additional legal requirements on preservation of corporate electronic records and emails can be expected to emerge in the future which must be factored into risk management practices.

4. OBJECTIVES OF CORPORATE INTERNET USE POLICIES

While preserving the confidentiality of internal operations, proprietary information and confidential client data, and avoiding legal liability from inadvertent, unauthorized or harmful acts of employees are primary goals for corporate email and internet use policies, they are not the only goals.

Corporations must also factor in other objectives not always consistent with limiting legal liability.

4.1 Reducing Lost Productivity

The concern among many businessmen from about 2000 was that allowing internet access in the workplace could result in a great increase in employee non-work activities. Available content on the internet has expanded far beyond TV fare since 2000 to include Facebook, streaming video and music sites, fantasy sports teams, on-line shopping, eBay, financial web sites and bank account access, news feeds, blogs and Twitter. Clearly, excessive employee non-work internet use during working hours can impose significant costs on a company; one source cites productivity loss as the top reason for instituting an “acceptable use policy” (AUP) for company email and internet (Smith, 2013). Also, employee perceptions that “everyone” is engaging in non-work-related email and internet use can rapidly spread. However, employees increasingly reject the idea of strictly defined “work” and “non-work” hours, believing they can be more productive engaging in company business at any time and from any place—on devices that they choose.

4.2 Protecting Tangible and Intangible Assets

Increasingly sophisticated hackers are constantly developing tools to penetrate corporate networks—almost always to the potential detriment of the company and its clients. They may be working for criminal enterprises, or for competitors or foreign governments, but their goal is the same—to gather as much valuable information for as long as possible. Citibank and Sony are only two of the largest and best-known victims of such attacks. Email remains the most popular way to introduce malware into corporate networks (Cisco, 2013).

4.3 Controlling Internet Costs

Many non-business internet uses (e.g., streaming video, movies and music downloads, and internet music and television feeds) are “bandwidth hogs”. While these applications may not directly cost the corporation, their cumulative use can easily consume a substantial portion of a corporation’s available bandwidth, which can require major expenses to expand the corporation’s network capabilities.

4.4 Attracting Talented Employees

If human capital is a company’s most valuable asset, avoiding unnecessary barriers to attracting the best future employees may require considerable adaptations in a corporation’s internet use and access policies. CISCO argues that preventing or limiting employee access to social media can put companies at a competitive disadvantage, and that by accepting social media, companies

provide their employees with the tools—and the culture—to be more productive, innovative and competitive.

5. WHAT SHOULD AN EFFECTIVE EMAIL AND INTERNET POLICY CONTAIN?

It is one thing to create an AUP for workplace email and internet but another—in a world where increasing numbers of employees consider access to the internet a right and claim they are willing to ignore or circumvent an employer’s internet use policies if they find them overly constraining—to enforce it.

5.1 Elements of an Acceptable Use Policy

No one is suggesting that not having an AUP is an option today. Every sizable business needs to have a formal risk management policy for email and internet use. Widespread agreement exists that the following elements need to be included:

5.1.1 Contractual Agreement

The AUP should be a written agreement with each employee and agent of the corporation having email and internet access; all employees should sign the AUP and acknowledge an understanding of its requirements as a prerequisite to gaining password access to the corporate network.

5.1.2 Corporate Ownership of Information

The AUP should clearly state that any information produced, collected or stored on the company’s email servers, internal networks and internet system is company property—even if the information was obtained from third-party web sites.

5.1.3 Monitoring

The AUP should indicate that the corporation reserves the right to monitor any and all employee access to and usage of its internal networks and internet system, including the volume of traffic and tracking web sites visited (although monitoring of specific content will not occur except in cases of a suspicion of improper behavior).

5.1.4 Retention

The AUP should indicate that all workplace emails and network transmissions are the property of the company, that they will be stored and retained indefinitely, and that the company has the right to demand access to any employee’s PCs, laptops, iPads or other electronic devices used for company business in the event of litigation or internal, regulatory or law enforcement

investigations in which data generated or stored on such devices may be potentially relevant.

5.1.5 Sanctions

Sanctions for violation of the email and internet use policy must be described and should include progressive steps, from initial verbal warnings up through dismissal and referral for criminal prosecution for repeated and/or serious offenses.

5.2 The Traditional View of Acceptable Use Policies

Differences of opinion exist over how to describe permitted and prohibited email and internet related activities. The traditional view (often advanced by vendors of solutions for creating and monitoring AUP policies) is that internet use policies should contain long and detailed lists of prohibited behaviors. For those following this “laundry list” approach, a list of prohibited email and internet activities often includes:

- Violating copyright laws or licensing agreements through unauthorized reproduction or distribution of copyrighted or protected materials.
- Using company computers to gain unauthorized access to external computer systems.
- Connecting unauthorized equipment to the company’s network.
- Making unauthorized attempts to circumvent data protection devices.
- Associating unapproved domain names with a company-owned IP address.
- Performing an act that interferes with the normal operation of any company hardware or software.
- Installing or running on any computer a program intended to damage or place excessive load on a computer system (e.g., viruses, Trojan horses or worms).
- Engaging in activities that waste or overload company computing resources.
- Using company resources for any non-work related commercial activity.
- Using email, social media or company-owned or sponsored hardware or services to harass or threaten others, or sending materials that might be deemed defamatory, derogatory, prejudicial, sexually offensive or unwanted.
- Initiating, propagating or perpetuating electronic chain letters.

- Sending inappropriate mass mailings, including “spamming”, “flooding” or “bombing”.
- Forging a user or machine identity electronically.
- Transmitting or reproducing materials that are slanderous or defamatory, that violate existing laws or regulations, or are otherwise inappropriate in a workplace environment.
- Transmitting images, text or internet links that could be considered lewd, obscene or sexually explicit.

5.3 An Alternative Risk-based View of Acceptable Use Policies

We suggest, however, that alternate risk management approaches may make more sense in many instances—focusing on controlling only those potential risks relevant to a corporation’s or organization’s specific activities. For example, a company engaged in design and manufacture of laptop computers necessarily works with critical proprietary information (e.g., R&D project designs, patent applications, trade secrets, manufacturing know how). Some of this information is owned and some is licensed from third parties—but all needs to be continuously protected to avoid potentially large economic damage and legal liability if improperly communicated, disclosed or accessed. The same need for protection of confidential client information would apply to law, accounting or consulting firms dealing with intellectual property, financial data, litigation, strategic acquisitions or other client information that requires protection against disclosure or inadvertent access. The same level of intellectual property safeguards would not be necessary for a pizza chain that provides online ordering and delivery scheduling. But the pizza business still needs to safeguard customer credit or debit card information, and both the computer manufacturer and the pizza business are equally exposed to potential workplace sexual harassment claims by employees resulting from use of company email or internet access.

Businesses embracing a “risk-focused” approach usually will retain the right to monitor employee compliance with specified or prohibited behaviors but may limit surveillance to activities at higher risk of employee misuse and spend more time making sure that employees understand the consequences of a failure to comply. Such more focused AUPs are more likely to be understood and followed—and to gain “buy-in” from a workforce that increasingly considers information security and liability avoidance as the IT department’s problem—and not theirs (Cisco, 2013).

While social media is gaining in importance in corporate activities, email remains the primary means of communication—and hence the primary focuses for corporate efforts to limit employee-caused legal liabilities or outside threats. To that end, many companies are using software such as CompuScan

that inserts disclaimers of liability for prohibited email use into all corporate email communications. However, such disclaimers are an imperfect shield at best—no court case has yet allowed a company to escape liability for damaging emails through use of a blanket disclaimer contained in the email. Disclaimers are more effective if they are targeted at specific areas of the business where liability is more likely—for an electrical contractor’s customer and vendor communications—“no bids or estimates are binding unless and until approved in writing by the VP for Finance”—and not simply attached to every email that company employees send.

6. STEPS IN IMPLEMENTING EFFECTIVE INTERNET USE POLICIES AND PROTECTING THE COMPANY FROM LEGAL LIABILITY

The changing state of the law on corporate liability for electronic communications and evolving employee attitudes and expectations make across-the-board recommendations for corporate internet and email use policies difficult—other than the recommendation every corporation or organization should have an AUP tailored to its specific workplace activities and risk exposures (indeed, the failure to have an AUP might be almost conclusive evidence of corporate negligence in litigation involving inappropriate employee emails or network activities). However, some general recommendations are possible:

- Analyze and understand the specific types of communications your company is actually sending and receiving and specific legal liabilities that are involved.
- Consult employees periodically as to how they are using the internet and email systems; do not simply rely on use statistics.
- Develop and mandate employee education programs (for both new hires and existing employees) about the potential for specific corporate liability for inappropriate communications.
- Implement monitoring software to follow all activities that the company decides to prohibit in its internet use policy (although it should be used only on a random basis or when cause for suspicion exists).

7. CONCLUSION

The continuing exposure to legal liability for corporate email and electronic communications and the importance of such communications in litigation and governmental investigations are unlikely to slow so long as corporate email and internet usage continue to gain importance in internal and external business

activities. But increasingly companies are moving to “risk-focused” instead of “laundry list” approaches to controlling internet and email use. To use this risk-focused approach, corporate risk management policies and employee educational activities for employee internet and email use need to be periodically revisited and revised, and corporations need to continuously seek employee “buy-in” and cooperation, to meet the most important legal exposures associated with specific corporate and employee activities.

REFERENCES

- CFO Journal. (2013). The Morning Ledger: CFOs seek security from cybercrime. *The Wall Street Journal*, August 13 2013. Retrieved from <http://blogs.wsj.com/cfo/2013/08/13/the-morning-ledger-cfos-seek-security-from-cybercrime/> on August 21, 2013.
- Cisco Systems. (2013). Cisco 2011 annual security report. Retrieved from http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2011.pdf (pp. 6-8) on May 21, 2013.
- Compuscan. (2013). Email disclaimer. Retrieved from <https://www.compuscan.co.za/about-us/132-email-disclaimer> on May 21, 2013.
- ITPro. (2013). Sony insurer doesn't want to pay for data breaches. Retrieved from <http://www.itpro.co.uk/635140/sony-insurer-doesn-t-want-to-pay-for-data-breaches> on May 21, 2013.
- Mailguard. (2013). Watch porn at work—a guide for employers and managers. Retrieved from <http://www.mailguard.com.au/blog/porn-at-work/> on May 21, 2013.
- National Legal Research Group, Inc. (2013). Internet acceptable use policies for law firms and other employers. Retrieved from <http://www.nlrg.com/internet-acceptable-use-policies-for-law-firms-and-other-employers/> on May 21, 2013.
- PBT Consulting. (2013). Research: Employees spend entirely too much time accessing the internet while at work. Retrieved from <http://tommytoy.typepad.com/tommy-toy-pbt-consultin/2010/09/research-employees-spending-entirely-too-much-time-surfing-the-web-while-at-work.html> on May 21, 2013.
- Pingdom. (2013). Internet 2011 in numbers. Retrieved from <http://royal.pingdom.com/2012/01/17/internet-2011-in-numbers/> on May 21, 2013.
- Ponemon Institute Research Report. (2013). Cost of data breach study: Global analysis. *Symantec Corporation*. Retrieved from

https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Pone_mon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf on September 2, 2013.

Radicati, Sara, and Hoang, Quoc. (2013). Email statistics report, 2011-2015. Retrieved from <http://www.radicati.com/wp/wp-content/uploads/2011/05/Email-Statistics-Report-2011-2015-Executive-Summary.pdf> on May 21, 2013.

Smith, Aaron. (2013). Citi–Millions stolen in May hack attack. Retrieved from http://money.cnn.com/2011/06/27/technology/citi_credit_card/index.htm on May 21, 2013.

Yarow, Jay. (2013). 107,000,000,000,000. Retrieved from http://articles.businessinsider.com/2011-01-14/tech/30078145_1_hours-of-video-uploaded-big-number-facebook on May 21, 2013.

Zubulake v. UBS Warburg [case study]. (2003).

ABOUT THE AUTHORS

John Ruhnka, JD, MBA, LLM, is a professor of law and ethics in the business school at the University of Colorado Denver.

Windham E. Loopenko, JD, MBA, is a member of the international business faculty in the business school at the University of Colorado Denver.

