Global Information Assurance Certification Paper

Email Acceptable Use: Balancing the Needs of the Organization and the Need to Comply with National Labor Relations Board Rulings.

GIAC (GLEG) Gold Certification

Author: Paul Hershberger, pjhersh13@gmail.com
Advisor: Barbara Filkins
Accepted: October 6, 2015

Abstract

Organizations strive to enact policies that protect intellectual property, including the reputation of their brand, and support a productive work environment, while at the same time respecting employee privacy and freedom of expression. Despite good intentions, organizations sometimes discover that their existing policies suddenly conflict with the legal system. Unexpected legal rulings can arise as authorities assess how technology changes the workplace. What is acceptable policy within an organization one day may be in violation of law the next. This paper examines National Labor Relations Board (NLRB) rulings regarding the use of email by employees for protected purposes such as union organizing and then presents an analysis of the implications of those rulings. Suggestions as to how policies and practices must evolve to meet the needs of the organization are made, while also complying with the NLRB's interpretation of employment law.

1. Introduction

In 1971 Ray Tomlinson was working as a computer engineer for Bolt Beranek and Newman, a high-technology research firm that served as a military contractor for DARPA. He developed a system for sending messages between computers using the @ symbol to identify the address of the sender and receiver of the message (Left, 2002). The first graphical user interface to email, Eudora, was created in 1988 followed by the release of Lotus Notes in 1989 (Left, 2002). With the release of commercial email management solutions the use of email as a form of business communication began to take hold. The use of email has become the most prevalent means of business communication, with over 108 billion business related emails sent and received every day in 2014 (The Radicanti Group, Inc., 2014). The use of email as a means of business communication has been a significant factor in the growth of a flexible work force allowing workers to collaborate around the globe working on schedules that are both flexible for the worker and timely for the business.

Although email communications has significant benefit to both the worker and the business it can also present serious risks to the individual as well as the business. Email use has expanded in not only business but also as a means of personal communication. The lines of email etiquette and acceptable use has often blurred and created situations where email communications within the business environment often take on a personal nature.

Businesses commonly publish acceptable use policies to help define guidelines for what is acceptable behavior when using business email systems. This paper examines the growth of email as a means of business communications, as well as the often conflicting requirements companies must address in defining acceptable use policies. Focusing on the National Labor Relations Board (NLRB) rulings on protected activities, such as union organizing, this paper explores how to balance email risk and acceptable use policy in order to achieve the objectives of the business while meeting the NLRB legal requirements.

2. Email Communications

2.1. Organizational imperatives for email

2.1.1. Flexibility

Arguably one of the most important benefits of email communications is flexibility. Email allows individuals to conduct business without regard for schedules, geographies, time zones or time of day from anywhere they can get an Internet connection. Combine that level of flexibility with the near instantaneous exchange of content between sender and receiver, and email can be seen as one of the most critical business systems within an organization. Although newer forms of communication such as social media and mobile text messaging services are raising in popularity, email is likely to remain a key part of business communications. Sara Radicati of the Radicati Group noted in her blog about her firm's *Email Statistics Report, 2012-2016*: "Over the next four years, we expect corporate email accounts to increase at a faster pace than consumer email accounts, as organizations continue to extend email services to employees who may not have had access to email in the past" (as cited in (Nelson, 2013, p. 4)). The flexibility, speed and ease of communication that email provides the business makes it a critical part of business operations.

2.1.2. Records Management

Fundamental principles of records management include establishing definitions of what constitutes business records, the relevant life span of the individual record and processes for identification, categorization, storage and eventual destruction of that record. The objective of records management is to ensure organizations retain relevant business documents, as required to meet their legal and regulatory obligations, while minimizing the retention of obsolete records. In a comprehensive analysis of document retention and destruction considerations the Notre Dame Law Review published an article that concludes:

> "In light of the expanding legal requirements imposed on business entities to retain documents for various periods of time, an increasing number of companies have recognized the practical and legal necessity of a comprehensive records management program. As business documents

> proliferate, the adoption and proper administration of such a program have become essential to the cost-efficient operation of a company and to the avoidance of practical, legal and ethical difficulties (Fedders & Guttenplan, 1980, p. 64)."

The continuing expansion of email as a form of business communications continues to push the limits of record management programs as organizations struggle to keep up with the growing volumes of information to sift through and manage.

2.1.3. Legal Hold and E-Discovery

The ability to comply with legal hold requirements and e-discovery orders is a growing concern for organizations. A recent article published in the Information Management Journal (Information Management Journal, 2014) discusses three key trends in e-discovery: 1) Sanctions for violating discovery orders are growing; 2) More courts are using their power to define guidelines for discovery efforts; and 3) New tools to enable e-discovery are continually expanding. The rules for e-discovery within the scope of the United States Courts are established within the Federal Rules of Civil Procedure (FRCP).

The FRCP Title V, Rule 34 states:

> In General. A party may serve on any other party a request within the scope of Rule 26(b):
>
> (1) to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party's possession, custody, or control:
>
> (A) any designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form (Cornell University Law School).

Essentially the rule places a requirement on organization to retain and produce to the courts any relevant content requested of it, within the scope of any civil proceedings in

the United States District Courts. As email continues to expand as a means of business communication, it is likely to remain a primary focus of e-discovery efforts.

2.1.4. Limiting high risk individual behaviors

Although email is an enabler of business operations and provides a high level of flexibility to the individual and the organization, it comes with risk. Once an email is sent, the sender has very little control over what happens with the message or how it is interpreted by the recipient. Even when a user takes action to delete email messages, those messages are often retrievable through forensic investigation. Email communications can create a perpetual record of high risk individual behaviors that can negatively impact the broader organization. Whether intentional, inadvertent, or otherwise unintended, email communications can become a significant risk. Accordingly, organizations strive to limit the amount of risk they face.

2.2. How email becomes a risk to an organization

Email is not intrinsically a risk to an organization in and of itself. When human behavior is introduced into the equation, the risk emerges as a new twist on that old problem, human behavior. Email communications can trigger behaviors in individuals that would otherwise remain restrained within the context of more personal direct contact. This behavior can be attributed to the reduction of social contextual cues which can increase group polarization.

Lee Sproull and Sara Kiesler examined the use of email within an organization and how the reduction of social context influences that communication (Sproull & Kiesler, 1986). A key finding from their research is that email provides relatively weak social context cues. The lack of social context can lead to communications that are more self-centered with people overestimating their own contribution to communications. Their research also concluded that people are more likely to behave irresponsibly through email than in face-to-face conversations and that people prefer to send bad news through email.

Another behavior that increases the risk associated with email is group polarization. Group polarization is defined as "A phenomenon wherein the decisions and opinions of people in a group setting become more extreme than their actual, privately

held beliefs" (Grinnell, 2009). A 2002 study into the effects of Computer Mediated Communication (CMC), such as email, on group polarization showed that the removal of visual cues or the perception of anonymity associated with CMC increased group polarization (Choon-Ling, Tan, & Kwok-Kee, 2002). The research went on to conclude that the perception of anonymity associated with CMC causes people to engage in more one-upmanship behavior which in turn contributed to the increased group polarization.

The risk associated with email continues to be witnessed in the courts and public forums alike with implications impacting both individuals and organizations. In 2006 a six-term congressman Rep. Mark Foley resigned amidst a scandal evidenced by inappropriate email communications with under-aged congressional staff members working under the Congressional Page program (Babington & Weisman, 2006). The 2014 hacking of Sony Pictures Entertainment included details of senior executive email communications being published on the Internet, exposing embarrassing racially slanderous exchanges as well as details of gender-based pay inequities at Sony (Howard, 2014). Scandals and court cases focusing on content of emails are seemingly endless from the ongoing Hillary Clinton email use scandal and the General Motors recall of 2014 to the conviction, and subsequent overturn, of Arthur Andersen for obstruction of justice.

The message is clear, email is a critical tool for the conduct of business and a continually growing means of personal and professional interaction within organizations. However there are serious risks that must be understood and managed appropriately as well.

2.3. Acceptable use policies

Since the early days of email use within organizations, the need for principles to guide behavior and promote acceptable use has been evident. James Gaskin wrote in a 1998 article (Gaskin, 1998) "The job of the acceptable use policy is to explain what the company considers acceptable Internet and/or computer use and behavior." Acceptable use policies are generally the means for defining those guidelines for what is acceptable use of technology and what actions should be considered inappropriate within an organization. When developing acceptable use policies it can be a natural progression to

try and reduce the risk to the organization to as low a level as possible. The need to reduce risk can result in a very restrictive policy with extremely narrow parameters of acceptable behavior. Though well intended, a narrowly defined scope of acceptable use, if not consistently applied and enforced, may create additional exposure to the organization.

3. National Labor Relations Board Rulings

The National Labor Relations Act, also known as the Wagner Bill, was signed into law by President Roosevelt on July 5, 1935. The Wagner Bill established the National Labor Relations Board (NLRB) to enforce employee rights (National Labor Relations Board). Since its inception, the NLRB has experienced several changes and today is comprised of a five member board that acts as a quasi-judicial body. The NLRB works to protect the rights of private sector employees to join together in collective bargaining activities in order to improve wages and working conditions (National Labor Relations Board).

Although the NLRB has heard over 500 appellate court cases and published over 2,000 decisions since 2005 (National Labor Relations Board), two recent cases stand out due to the implication as to the development of acceptable use policies. The rulings in the 2007 Register-Guard and the 2014 Purple Communications cases highlight the challenges of developing and implementing acceptable use policies that achieve the many objectives of the organization.

3.1. The Register-Guard and Eugene Newspaper Guild, CWA Local 37194

The Register-Guard is a family-owned Eugene Oregon based newspaper company with a history dating back to 1867 (The Register-Guard). In a 2007 NLRB Decision, (National Labor Realtions Board, 2007), the NLRB considered several issues related to the use of The Register-Guard company email systems for the purposes of National Labor Relations Act ("the Act") Section 7 related activities along with Section 8(a)(3) and (1) of the Act. Section 7 of the Act guarantees employees "the right to self-organize,

to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid to protection," as well as the right *"to refrain from any of all such activities."* Section 8(a) (1) of the Act makes it an unfair labor practice *"to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in Section 7"* of the Act (National Labor Relations Board).

The complaint against the Register-Guard centered on enforcement of a "Communications System Policy" (CSP) implemented by the company in October 1996. Among other stipulations the CSP stated:

> *Company communications systems and the equipment used to operate the communication systems are owned and provided by the Company to assist in the conduct of the business of the Register-Guard. Communications systems are not to be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations.*

In May and August 2000, Suzi Prozanski, a Register-Guard employee and the Communications Workers of America (CWA) Local 37194 president received two written warnings for sending three union-related emails in violation of the company's CSP. Subsequent to the warnings, in the course of labor negotiations, the company proposed incorporating elements of the CSP into the union contract which would prohibit the use of company email systems to conduct union business. The union representatives argued in front of the NLRB that the company insisted on the language which in turn represented an illegal subject in violation of section 8 of the Act.

After consideration of the facts in the case as well as extensive review of prior case law, the NLRB ruled that *"employees have no statutory right to use the Respondent's (The Register-Guard) email system for Section 7 purposes"* (National Labor Realtions Board, 2007, p. 1110). The decision by the NLRB found that the company had a consistent record of enforcing the CSP, as it relates to nonjob-related solicitations for employees to engage in or support social, political, religious or other outside organizations; however, they tolerated nonjob-related email communications for social gatherings, jokes, baby announcements and other personal items.

The NLRB ruled that the company had acted within the acceptable boundaries by enforcing their CSP with regard to two of the three email communications. With regard to the third email (sent May 4th 2000), they found that the message sent by Ms. Prozanski was informational in nature and did not constitute a "nonjob-related solicitation." Additionally since the company had tolerated nonjob-related email communications that their discipline of Ms. Prozanski for the May 4th email was discriminatory in nature and violated her rights under Section 7 of the Act.

In this landmark case the NLRB affirmed the rights of the organization to establish policy that restricts the use of email for nonjob-related purposes, going on to show how the consistent application and enforcement of that policy is critical to achieving the intent of the policy. The ruling essentially states that the organization has the right to establish restrictive policies, as long as they consistently enforce the policy.

Setting the stage for future debate of decision, the two NLRB members opened their dissent by stating:

> *Only a Board that has been asleep for the past 20 years could fail to recognize the e-mail has revolutionized communication both within and outside the workplace. In 2007, on cannot reasonably contend, as the majority does, that an e-mail system is a piece of communications equipment to be treated just as the law treats bulletin boards, telephones, and pieces of scrap paper.*

They went on to argue that email has created a new kind of community gathering place that enables individuals to exchange ideas and collaborate in a way the legal system was not fully recognizing. The arguments raised by the dissenting parties showed that this was clearly a topic that would raise to the surface again, and that it did.

3.2. Purple Communications, Inc. and the Communications Workers of America

The NLRB once again addressed the issue of email communications and Section 7 rights in 2014 as a result of a case filed December 2012 in Long Beach California. On December 11, 2014 the NLRB published a ruling in the case of Purple Communication, Inc. and Communications Workers of America, AFL0CIO (National Labor Relations Board, 2014). Similar to the Register-Guard case, the Purple Communications case

centered on the company's electronic communications policy. Purple Communications is a company that specializes in providing communications solutions for the hearing impaired, servicing individuals and companies alike. Since June 2012 the company maintained an employee handbook that contained an electronic communications policy that stated:

> *INTERNET, INTRANET, VOICEMAIL AND ELECTRONIC COMMUNICATION POLICY*
> *Computers, laptops, internet access, voicemail, electronic mail (email), Blackberry, cellular telephones and/or other Company equipment is provided and maintained by the {sic} Purple to facilitate Company business. All information and messages stored, sent and received on these systems are the sole and exclusive property of the Company, regardless of the author or recipient. All such equipment and access should be used for business purposes only.*
> *.....*
> ***Prohibited activities***
> *Employees are strictly prohibited from using the computer, internet, voicemail and email systems, and other Company equipment in connection with any of the following activities:*
> *.....*
> *2. Engaging in activities on behalf of organizations or persons with no professional or business affiliation with the Company.*
> *.....*
> *5. Sending uninvited email of a personal nature.*

A complaint was filed that argued the company's policy interfered with union members' freedom of choice in union board elections at seven of the company's call centers and that the policy represented an unfair labor practice. The case was essentially a referendum of the Register-Guard decision and this time the NLRB took a completely different view. In the conclusion section of the decisions the majority stated (National Labor Relations Board, 2014, p. 17):

> *The Register Guard dissenters viewed the decision as confirming that the Board was 'the Rip Van Winkle of administrative agencies,' by 'fail[ing] to recognize that e-mail ha[d] revolutionized communications both within and outside the workplace' and by unreasonably contending 'that an e-mail system is a piece of communications equipment to be*

> *treated just as the law treats bulletin boards, telephones, and pieces of scrap paper.'..... In overruling the Register Guard, we seek to make '[n]ational labor policy... responsive to the enormous technological changes that are taking place in our society."*

The NLRB reversed the Register-Guard ruling based on the argument that email is a common form of workplace communications that has evolved dramatically over the years to the extent that it must be included in the protections of Section 7 of the Act. The decision continues to stipulate boundaries of use specifically noting that there is an expectation that protected activities under Section 7 using company email systems would be conducted on non-work time. Additionally, the decision affirms the rights of the organization to monitor email communications in support of policy enforcement, as long as those monitoring activities are not performed in a manner that targets or emphasizes the monitoring of protected activities. The decision clarifies that the use of company email for Section 7 activities is a protected right for those employees provided access to company email systems as a normal course of their job responsibilities. The ruling does not create a requirement for the company to provide email system access to employees who would not otherwise require such access for business purposes. With this ruling, the NLRB validated and substantially adopted the dissenting opinion in the Register-Guard decision.

Although the Purple Communications decision stands today, the dissenting opinions may point to future challenges to the decision. NLRB member Philip A. Miscimarra argues that the decision assumes that, by limiting the use of company-owned email systems for Section 7 activities, the company is creating an unreasonable impediment to self-organizing. The dissent highlights the proliferation of access to personal email accounts and social media, as strong viable means communications for self-organization and how they are equal or greater alternatives available to employees for the purpose of Section 7 activities.

With the decisions in the Register-Guard and Purple Communications cases, it is clear to see that policies governing the use of electronic communications must be carefully designed, communicated and consistently enforced. Additionally the rapidly evolving nature of technology and the expansion of technology into every aspect of life

will continue to challenge the interpretation of law. Policy and practices within organizations need to show an understanding of the multiple potential implications and ensure they are adaptable to changes as they come.

4. Acceptable Use Policy Analysis and Advice

It seems as if acceptable use policies were created just after the Internet and the form, content and enforcement has been debated ever since. There is little argument that an acceptable use policy is needed, but how they are crafted, communicated and enforced can either manage your risk or create more risk to the organization. It may seem like a simple task to sit down and write a policy that defines all of the behaviors that will not be tolerated and set a tone of "thou shall not under any circumstances"; however creating a policy that truly manages the risk to the organization is not as simple as laying down the law on what a person should under no circumstances ever do.

Every word in an acceptable use policy matters and can influence the way that policy is interpreted, implemented and enforced. The wording of an acceptable use policy should be clear and aligned with the intent of the policy. In the Register-Guard case, Suzi Prozanski was subject to multiple formal disciplinary actions by her employer for the violation of their acceptable use policy. The company had determined that three email messages she sent violated the policy. When the NLRB reviewed the case they found that the company acted inappropriately with regard to one of the three emails. The heart of the debate by the NLRB focused on a section of their policy that stated:

> *Company communications systems and the equipment used to operate the communication systems are owned and provided by the Company to assist in the conduct of the business of the Register-Guard. Communications systems are not to be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations.*

When evaluating the section of the Register-Guard policy it contains several terms that significantly limit the scope of the policy. The first limiting factors are associated with organizational elements specifically noting commercial ventures, religious or political causes and outside organizations. By defining a list of organization

types that could constitute unauthorized communications, the policy could work against the company when undefined organization types are encountered. In the Register-Guard policy they continued to add a catch all phrase of 'non-job-related' to the end of the definition which can be helpful when situations arise that don't closely align with the definition in the policy. The most significant limitation in the policy and the one that was used in the final ruling were the words ‘solicit’ and ‘solicitations.’ When the NLRB ruled in this case they made it clear that the policy was reasonable and sound; however, with the limitation of the policy to be solicitations, the policy did not prohibit one of the three emails that were cause for the disciplinary actions against Ms. Prozanski. Because the policy language focused on solicitations, the NLRB examined how the company treated other non-work related email communications that were not considered solicitations. They found that the company commonly allowed non-work related emails that would not be considered solicitations. The NLRB ultimately ruled against the company with regard to the email that was not considered a solicitation based on the policy language and the company enforcement history. Creating tightly defined criteria within an acceptable use policy can help with clarity for the target audience; however, it can simultaneously restrict the latitude to enforce policy when situations do not exactly align with the definition in the policy.

When creating an acceptable use policy it remains important to define boundaries between what is and is not considered acceptable actions and how those boundaries are defined critical. When establishing boundaries in policy consider language that supports a level of ambiguity and allows for judgment based on the situation at hand. Consider the use of terms such as 'may, could, and should' over 'must, will, shall or shall not', to define boundaries that are flexible in nature. When defined lists are needed in the policy consider including phrases such as 'including but not limited to' to help open the criteria up and communicate that the defined list is not all inclusive. Creating soft boundaries may increase the effort by the organization to clearly interpret and enforce the policy; however it can be useful in supporting situations that have not been anticipated at the time of policy creation.

An acceptable use policy is only as effective as the organization's ability to enforce the policy. When writing an acceptable use policy it can be tempting to create a

series of mandates that are clear, rigid and absolute. The absolute nature of an acceptable use policy can provide clear authority to the organization but it can also limit judgment and flexibility in policy enforcement. The creation of absolute conditions can occur when policy is written using terms such as 'must, will, shall, shall not' along with similarly definitive terms.

Establishing absolute conditions in the acceptable use policy can create a significant burden on the organization as it can set an expectation of absolute enforcement. For instance if the acceptable use policy creates an expectation that email must not be used for purposes other than the conduct of company business, can the organization effectively monitor email use at a level that supports enforcement? If so, are the resources required to enforce that policy requirement justified by the business risk? One of the overall objectives of an acceptable use policy is to manage risk to the organization. Managing risk to an acceptable level involves establishing a balance between the cost of managing the risk with the potential impact of realizing the risk. Creating a policy that is overly restrictive and definitive in nature can set an expectation of enforcement that is misaligned with actual risk.

When creating an acceptable use policy consider first evaluating the risk to the organization, the potential impact of the risk and the level of risk the organization can accept. Understanding the risk tolerance can help create a policy that is aligned with that risk tolerance and can be effectively enforced. Understanding that an organization will accept risk to a certain level, the policy should be written to define tolerance levels of use rather than definitive statements of what is acceptable and unacceptable. Tolerance levels can be defined through policy statements acknowledging that some level of unacceptable use will occur, but the organization can only accept a certain level of risk. The policy should define the level of risk tolerable within the policy and further clarify that there are often limitations on the ability to monitor and enforce compliance. Communicating the limitations in the ability to enforce compliance may be accomplished through the use of qualifying statements such as ‘we strive to’, ‘we aspire to’, or ‘we intend to’. Acknowledging limitations in enforcement can support the organization's effort to manage the cost of compliance while meeting their risk management objectives.

Once a policy is established and expectations of the organization and the individuals within that organization are established, monitoring and enforcement has to follow. Consistent enforcement of the policy is critical to accomplishing the goals of the policy. In the Register-Guard case the NLRB ruled against the organization in their enforcement of policy. The basis of the ruling centered on the evaluation of consistency in enforcement of the policy. In evaluating the issue, the NLRB compared the email considered as unacceptable by the company with other similar emails sent and received by other employees of the organization. The NLRB determined that the enforcement was not consistent and in turn that the company selectively enforced the policy to limit activities protected under section 7 of the Act.

A policy that includes soft boundaries and relies on judgment in the monitoring and enforcement of that policy, consistency can be difficult. To help with consistency of enforcement consideration of how legal practices work and the way the courts track legal precedence may offer solution. Consider creating a library of enforcement actions, similar to a legal library, then track the circumstances around policy enforcement across the organization and establish enforcement precedence that can be leveraged in future enforcement actions. The process of tracking enforcement actions can manage the risk of inconsistency and facilitate an enforcement effort that is effective and achieves the objectives of the policy.

Once the acceptable use policy is written, well defined and consistently enforced there's still more to consider because what is legal today may not be tomorrow. The desire may be to create policy that will stand the test of time and not require revision, but that is not always a realistic expectation. Technology is changing at an incredible rate and the legal system is evolving as well. With the dynamics of change the organization cannot lose sight of how those changes may impact the validity and legality of their policies and enforcement efforts. Within the narrow scope of the two cases examined, the question of acceptable use policy as it relates to the conduct and restrictions to Section 7 protected activities shows how the legal system can change over time. A decision by the NLRB in 2007 cleared the way for organizations to limit the use of company email systems for Section 7 protected activities, only to be reversed by the same board in 2014. In both cases the NLRB went to great lengths to examine the use of email

and technology as a form of communications from a business and personal perspective, considering how that technology has influenced social interaction and collaboration across individuals and organizations.

The process for developing, publishing and maintaining policies should incorporate review and evaluation of factors such as legal precedence, technology trends, social collaboration trends, and changes to the organization operational and risk management needs. These factors can influence the need to evolve policy to help the organization effectively manage risk while remaining within the bounds of legal acceptability.

5. Conclusions

Acceptable use policy is an important tool for an organization to provide guidance to technology users on what it and is not acceptable behavior. Much like societal norms of behavior, the line between what is acceptable and not is often not clearly defined and it can change over time. When establishing an acceptable use policy and the programs supporting that policy, organizations should begin with understanding the level of risk they are willing to tolerate and establish a risk tolerance that policy can be aligned to. Using the risk tolerance the acceptable use policy should focus on providing guidance to the organization around the boundaries of what is acceptable and when behaviors may come into conflict with the boundaries of risk tolerance. When writing the policy special care should be given to the language use to define and communicate the boundaries of risk tolerance. The language in the actual policy should be carefully chosen to be clear enough to the individuals within the organization, while remaining flexible enough to allow the organization to evaluate each potential violation and apply judgment in when and how the policy is enforced. The boundaries of what is beyond risk tolerance should be carefully defined in a manner that the organization is capable of monitoring and enforcing those boundaries.

Maintaining consistency in policy enforcement is also critical to the long term success of the policy and the goal of mitigating risk to the organization. Inconsistency in enforcement can create additional risk to the organization and can result in financial and

reputational losses. Enforcement actions should be documented and used as references for future enforcement actions to assist with the objective of consistency. Finally the organization should remain conscious of the evolving nature of technology, social interaction and legal precedence that can necessitate changes to the policy and their associated practices.

Keeping these guidelines in mind when developing and maintaining acceptable use policy can help support the risk management objectives of the organization and sustain an acceptable use policy that is effective for the organization and accepted by the user community alike.

References

Babington, C., & Weisman, J. (2006, September 30). *Rep. Foley Quits In Page Scandal*. Retrieved June 19, 2015, from Washington Post Politics: http://www.washingtonpost.com/wp-dyn/content/article/2006/09/29/AR2006092901574.html

Choon-Ling, S., Tan, B. C., & Kwok-Kee, W. (2002, March 1). Group Polarization and Computer-Mediated Communication: Effects of Communication Cues, Social Presence, and Anonymity. *Information Systems Research, 13*(1), 70-90.

Cornell University Law School. (n.d.). *Legal Information Institute*. Retrieved May 29, 2015, from Cornell University Law School: https://www.law.cornell.edu/rules/frcp#Form_6_1_target

Fedders, J. M., & Guttenplan, L. H. (1980, 10 1). Document Retention and Destruction: Practicle, Legal, and Ethical Considerations. *Notre Dame Law Review, 56*(1).

Gaskin, J. E. (1998). Internet acceptable useage policies. *Information Systems Management, 15*(2), 20.

Grinnell, R. (2009, Jan 10). *Group Polarization*. Retrieved May 31, 2015, from PshychCentral: http://psychcentral.com/encyclopedia/2009/group-polarization/

Howard, A. (2014, December 11). *5 of the most shickgin Sony hack revelations*. Retrieved June 19, 2015, from MSNBC Society: http://www.msnbc.com/msnbc/5-the-most-shocking-sony-hack-revelations

Information Management Journal. (2014, November 1). Notable Trends in E-Discovery. *Information Management Journal*, 17.

Left, S. (2002, March 13). *Email timeline*. Retrieved May 9, 2015, from theguardian: http://www.theguardian.com/technology/2002/mar/13/internetnews

National Labor Realtions Board. (2007, Dec 16). *National Labor Relations Board.* Retrieved May 2, 2015, from Board Decisions: http://apps.nlrb.gov/link/document.aspx/09031d45801ab7d6

National Labor Relations Board. (2014, Dec 11). *Board Decisions.* Retrieved May 2, 2015, from National Labor Relations Board: http://apps.nlrb.gov/link/document.aspx/09031d45819e22c9

National Labor Relations Board. (n.d.). *Graphs & Data*. Retrieved June 28, 2015, from National Labor Relations Board: http://www.nlrb.gov/news-outreach/graphs-data

National Labor Relations Board. (n.d.). *Interfering with employee rights (Section 7 & 8(a)(1)).* Retrieved June 28, 2015, from National Labor Relations Board: http://www.nlrb.gov/rights-we-protect/whats-law/employers/interfering-employee-rights-section-7-8a1

National Labor Relations Board. (n.d.). *The NLB and "The Old NLRB"*. Retrieved June 19, 2015, from National Labor Relations Board: http://www.nlrb.gov/who-we-are/our-history/1935-passage-wagner-act

National Labor Relations Board. (n.d.). *Who We Are*. Retrieved June 19, 2015, from National Labor Realtions Board: http://www.nlrb.gov/who-we-are

Paul Hershberger, pjhersh13@gmail.com

Nelson, R. (2013, May). Email in a Social-Media World. *EE: Evaluation Engineering*, p. 4.

Sproull, L., & Kiesler, S. (1986, Nov 11). Reducing Social Context Cues: Electronic Mail in Organizational Communication. *Management Science, 32*(11), 1492-1512.

The Radicanti Group, Inc. (2014). *Email Stetistics Report, 2014-2018.* The Radicanti Group, Inc. Palo Alto: The Radicanti Group, Inc.

The Register-Guard. (n.d.). *About the Register-Guard*. Retrieved June 28, 2015, from The Register-Gurad: http://projects.registerguard.com/pages/about-the-register-guard/