Title: Are Organizations Ready For the Electronic Renaissance in Communication?
Email Monitoring & Privacy Issues.
Authors: Jim Kates & Philip Whited of the IntraSec Corporation

ABSTRACT
In the last thirty years we have witnessed the coming of the computer age and a renaissance of communication. The role of the computer is vital to the everyday workings of modern society and has had a profound effect in the corporate world facilitating communication. It has given businesses the ability to manage their communications more efficiently and increasing, through better communication, employee productivity immensely. Electronic mail, or as most popularly known as Email, in itself has increased the usage of computers by becoming one of the most heavily used applications residing in corporate information systems. Within this renaissance has arisen concerns of how we properly use this new form of communication and learn new mores to adapt to this technological culture.

Communication in the past relied heavily on verbal interfacing. With the use of email in the office skyrocketing in the last five years, the electronic media is a critical piece of the organization's communication structure. According to recent statistics, 90 percent of large companies, 64 percent of midsize companies, and 42 percent of small businesses use email. This results in almost 3 billion messages transmitted every month, which has increased from 508 million per month in 1994. The reasons for this increase are clear. Email communication improves productivity in the workplace because of the speed and responsiveness with which communications take place. Instead of trying to communicate through meetings or phone calls, employees can now simply communicate their ideas through email quickly and efficiently. Email is becoming another form of faceless communication that our society is quickly adapting.

A hypocrisy exist within this more anonymous act of communication, in that people feel a false of privacy or secretive communiqué that comes with tangible written mail. The real fact is that within this improved technology, employees do not have the same level of assurance of privacy that common hand delivered mail tends to provide. To understand the problem we need to examine the difference between the handling of physical mail and its electronic counterpart. First of all, laws and statutes may protect letters handled by government agencies[1]. Secondly, even physical mail handled by non-government agencies, like FEDEX or UPS have legal protections associated with them[2]. However, because this technology is relatively new, legality is vague when governing employees and employers concerning email privacy. The following pages will describe some of the

[1] Title 18, Chapter 83 of US code

[2] All rights concerning privacy are contractual. There are no US laws governing these agencies regarding your package privacy. They reserve the right to open any package they process.

present United States policy as espoused by corporations regarding email privacy. Then we will discuss both proposed and enacted legislation, and outline some of the recent cases that are used as precedent in courtroom decisions.

INTRODUCTION

In addressing the real issues that have arisen due to the recent increase in electronic communications there are many conflicting issues that must be taken into account. One example is an employee's expectation of privacy in the workplace within the framework of e-communications. People assume that Email, like U.S. postal mail, is protected from prying eyes. This is the quintessential people issue, which has fueled this entire debate. On the flip side is disclosure of confidential information. Many organizations feel the content of their email may negatively affect their business if inappropriately used. Thus they feel the need to control access to it. These conflicting issues have culminated into a heated debate between employers and employees concerning their rights. This conflict can be seen in the summary below:

Employees	Employers
✓ Feel that they deserve some allowance of privacy in the workplace.	✓ Feel that the use of corporate resources deems anything produced as proprietary.
✓ Feel that constant monitoring violates privacy laws as set by United States Legislature.	✓ Feel that corporate resources should be used for business purposes only and monitoring is a way of enforcing this.
✓ Feel a lack of trust by the employer if monitoring is deemed necessary.	✓ Feel they need to protect confidential and privileged information from outsiders or competitors.

The employee concerns may grow considering the fact that companies may be increasing their use of Email monitoring. One study by the ACLU stated, "20 million workers have their email, computer files, and voicemail searched by their employers. In industries such as telecommunications, insurance, and banking, it is estimated that 88% of employees are subject to monitoring". Another source, The Society for Human Resource Management, took a random sampling of their members and found that 36% of the respondents said employers access their email records for business purposes and security while 7.7% conduct random reviews. How wide spread email monitoring exists is in question, since it can be done surreptitiously. An interesting fact is that despite the potential for a large amount of employees being monitored, only 36 % of companies have defined email

policies that may legally permit them to do so. This has left many companies unprepared for legal confrontation with employees when they eventually arise and has resulted in many gray areas concerning this issue.

Even with those companies that have established Email policies, they are often obscure and weakly defined. Furthermore, companies with good policies should not rely on them alone, when monitoring email is planned or expected. Policies should be supplemented by other mechanisms to increase their effectiveness and reduce the legal risks. A few examples of the elements that can supplement an Email policy might be;

1. A short newsletter or management briefing that informs employees of the monitoring. This would be strengthened by a banner message on the network identifying the possibility that Email may be periodically monitored for business purposes.
2. Having a new employee sign consent forms that allow monitoring.
3. Reinforcing in meetings that the corporation is the sole provider of the email system and owns information within that system.

In this last example there is an explicit implication involved with being the provider of an Email system. In the Electronic Communications Protection Act, ECPA, a provider is excused from the legislation and allowed full monitoring privileges. By mentioning this fact the employer may be excused from that portion of the law that restricts monitoring.

On the other hand, the employee would have no clue that he/she was open to monitoring unless they had prior knowledge of the law or were informed by the employer. The laws governing this new technology are in there fledgling state. If not careful, some companies will attempt to try and use obscure policies to slip through the loopholes in the enacted legislature. These policies while they may be legal, may be seen by employees as inappropriate or misleading. Most organization should look to avoid that and provide an open, honest approach to monitoring activities.

MONITORING LAWS

In addressing the above mentioned issues one must look at the enacted legislature that would come into play and the rationale behind how decisions are made by courtroom officials.

An Employee's right to e-mail privacy is largely governed by state tort law[3]. There are four distinct torts protecting the right to privacy: (1) unreasonable intrusion upon the seclusion of another; (2) misappropriation of another's name or likeness; (3) unreasonable publicity given to another's private life; (4) publicity that unreasonably places another in a false light before the public. The tort most relevant to email privacy expected from employers is the unreasonable intrusion upon the seclusion of another.

[3] Article 1, Section 23 Florida State Constitution

"Section 652B of the restatement on torts defines intrusion upon seclusion as intentionally intruding, physically or otherwise, upon the solitude or seclusion of another or his/her private affairs or concerns." To justify this tort the intrusion must be considered highly offensive to a reasonable person. It is usually found that electronic monitoring is a sufficient enough intrusion to warrant this tort. In determining whether or not an intrusion is considered "Highly Offensive" the court takes into account the circumstances around the intrusion, the context, the motives, the objectives as well as the expectation of privacy of the employee.

To balance both the needs of the employee and employer the court considers two requirements in its final decision. That the employee have a subjective expectation of privacy and that it is objectively reasonable. The Court uses this to then justify it ruling while considering the expectation of privacy by the employee to the justification of monitoring by the employer for business success.

In addition to the tort law mentioned above there are three enacted pieces of Federal legislature that may play a major role in the organization's decision-making process. The following three acts regularly appear when looking at precedents that are a result of disputes over e-privacy; Privacy for Consumer and Workers Act, The Electronic Communications Protection Act, and The Omnibus Crime Control and Safe Streets Act. Each of these acts addresses a different concern but at the same time may create loopholes for employers who would try to abuse their monitoring privilege.

The Privacy for Consumers and Workers Act was enacted to prevent the abuses of electronic monitoring[4] in the workplace. Some points of importance are that the employer must make aware the employee in writing that they are being monitored and must post this information in a conspicuous place so that all employees are reminded of such facts.

In addition the employer must provide the employee with:

1. The forms of electronic monitoring to be used.
2. The personal data to be collected.
3. The hours and days per calendar week that electronic monitoring will occur.
4. The use to be made of personal data collected.

[4] The term "electronic monitoring" means the collection, storage, analysis, or reporting of information concerning an individual's activities by means of a computer, electronic observation and supervision, telephone service observation, telephone call accounting, or other form of visual, auditory, or computer-based technology that is conducted by any method other than direct observation by another person, including the following methods: Transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature which are transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic, or photo-optical system.

5. Interpretation of printouts of statistics or other records of information collected through electronic monitoring if the interpretation or records may affect one or more of the employer's employees.
6. Existing production standards and work performance expectations.
7. Methods for determining production standards and work performance expectations based on electronic monitoring statistics if the methods affect the employees.
8. A description of the electronic monitoring.
9. A description of the exception that is authorized under section 5(c)(1) to be undertaken without notice.

The exception in part nine allows employers to monitor without notice if they believe the commission of a crime can be prevented. In addition to this exception there is a subsection 5(c)(1) that allows monitoring of an employee without notification if the employee is engaged or about to engage in conduct which (A) Violates criminal or civil law or constitutes willful gross misconduct; and (B) Has significant adverse affect involving economic loss or injury to the employer or employer's employees. Overall this act is intended to prevent employers from monitoring employee communications for unauthorized purposes or without taking proper channels to reduce the chance of misuse.

The next act The Electronic Communications Protection Act (ECPA) is an amended piece of legislation to the Omnibus Crime Control and Safe Streets Act. This act prevents unauthorized interception of wire and oral communications to include other forms of electronic communications. The ECPA makes it a federal crime for an individual to willfully intercept, access, disclose, or use another's wire, oral, or electric communication. This act has a very limited scope applying to those areas regarding interstate commerce. Arguably, email over a corporate LAN would not fit into the scope of this law because of the lack of effect on interstate commerce. However, it can be further argued that the law does apply because of the use of extranets and email systems that do travel over state lines. Because of this aspect a gray area rises in defining what is a truly internal network. In addition there are three exceptions to this law that allow for employers to monitor their network. They are the provider exception, the business exception, and the consent exception. All three of these exceptions allow for a complete monitoring if the right conditions apply.

The next act, which is brought into issues concerning electronic communications, is The Omnibus Crime Control and Safe Streets Act. As stated earlier this act was amended by the ECPA to address the issue of email. This act was enacted in 1968 and addressed the concern of many citizens about unauthorized wiretapping that might be occurring. This was a time when the FBI was heavily tapping phone lines and monitoring of individuals because of organized crime families and their dealings with illegal rackets. Innocent citizens felt that this monitoring was out of control and demanded that something be done about it. This act was the result and the scope of which wiretapping and surveillance was limited. It first made it illegal for non-law enforcement agents to eavesdrop. Secondly,

there were only certain situations in which law enforcement could monitor. They included investigations of bribery, kidnapping, robbery, murder, counterfeiting, fraud, narcotics, or conspiracy. Furthermore it can be done only as a last resort and it must be demonstrated that all other avenues were properly exhausted.

In addition to these specific laws, certain portions of the Bill of Rights have been interpreted to address these concerns. In particular they are the Fourth and Fifth Amendment. The Fourth amendment which guards against unreasonable searches and seizures and the Fifth Amendment which prevents the deprivation of property. These interpretations tend to only apply to government employed individuals though.

Even though there is a plethora of legislation focusing on this issue many employers have used the loopholes or exemptions that are built into the laws to continue monitoring employees. Each one of the pieces of federal legislation has a clause that grants exception. These clauses can be interpreted rather loosely to grant monitoring privileges to employers. In addition, the establishments of the torts to warrant intrusion are subjective in nature and are open to a wide range of interpretation.

ENCRYPTION

To combat this, employees have taken it upon themselves to restrict access to their electronic transmission. Through the use of encryption employees thwart the employers' ability to read what was is being transmitted. This in turn has raised another issue and has brought with it more proposed legislature focusing on this aspect. Presently there are four pieces of pending legislature that concentrate on the use of encryption by employees. They are as follows:

1. Security and Freedom Through Encryption Act (SAFE)
2. Encrypted Communications and Privacy Act of 1997
3. Secure Public Networks Act
4. Oxley-Manton Bill

The first three acts intend to provide for the rights of the employee in their unrestricted use of encryption, while the last bill hopes to create a clause in which a backdoor is always available for deciphering when it is requested. Because it is legal for employees to use encryption many employers are lobbying for laws banning or greatly restricting its use.

PRECEDENT

As I stated earlier, many companies do not have set policies regarding their networks and monitoring of employee email. And because the technology is relatively new, laws that concentrate on issues surrounding e-communications are obscurely defined and laden with loopholes. As a result of these blurred boundaries some employers have found themselves in court over the use of their networks and the rights of employees to privacy.

From these dockets several precedents have been set in the arena of e-communications. Notable court cases that have set the guidelines for future reference include:

1. **Bourke v. Nissan**
2. **Shoars v. Epson**
3. **Smyth v. Pillsbury**

The case of **Bourke v. Nissan** involved the transmission of sexually explicit emails over a corporate network. In this case Bonita Bourke sent some sexually explicit emails over the corporate network where she was employed by an Infiniti dealership. Because of her conduct Nissan Corporation reprimanded Ms. Bourke and her cohort. After a long protest towards the reprimand, Ms. Bourke resigned and her friend was terminated. As a result Ms. Bourke sued under the ECPA and Omnibus Crime Act. She felt that Nissan violated her right of privacy as an employee so she was due compensation. The court ruled that because Ms. Bourke signed a paper explicitly stating her intent to use corporate email for business purposes only, her actions were in direct violation of company policy. Also, she was aware that her emails were available to be read by her fellow employees, which negated her expectation of any right to privacy. As far as her claim under the Omnibus Crime Act, violation of this act requires intercepting emails in transmission. The emails Ms. Bourke sent were read from a stored location so Nissan was in no violation of said act. The court granted a summary judgement in favor of Nissan.

The case of **Shoars v. Epson** again involved the retrieval of stored email. In this case Alana Shoars was responsible for the training and support of her company's office email system. Through her training sessions she had informed all employees that their email messages remained private and confidential. Upon discovering that her supervisor was intercepting email messages and reading them, she demanded that he stop. After attaining a private email account that was inaccessible by her supervisor, she was fired for gross insubordination. In retaliation, she sued under the ECPA. The court rule that the retrieval of email did not constitute the "Tapping" of a telephone line in violation of the Penal Code. The court ruled in the favor of Epson.

In **Smyth v. Pillsbury**, the plaintiff, Michael A. Smyth, received certain email messages at home from his supervisor. In an exchange between them, Mr. Smyth made some rather offensive comments about some of his associates alluding to their poisonings. The company executives, who saw a printout of this message, terminated Mr. Smyth for inappropriate and unprofessional comments over the Defendant's email system. The plaintiff filed a wrongful discharge action claiming a violation of his right of privacy. In support of his claim the plaintiff alleged that the company assured him of his email privacy. The court ruled that because the plaintiff communicated an offensive comment over a corporate wide network that he surrenders any right to privacy that he might

expect. In addition, the court found that it was in the best interest of the company to monitor for such inappropriate and unprofessional comments sighting safety reasons.

These three cases explicitly show how much privacy employees should expect when using a company email system. In each of the cases, none of the employees signed papers consenting to monitoring. Nor were they informed that the monitoring would take place. In two of the cases the employees were even informed that their mail would be kept confidential. The policies, as defined by these court dockets, seem to be in direct violation of the Privacy for Consumers and Workers act. However, the rulings were all in favor of the employer.

The precedent set by these judgements sends a clear message to employees that use corporate networks. It is up to the company to decide on its policy when regulating email use. Employees should not count on pursuing legal action using the enacted legislation or establishment of torts. From the laws mentioned above, little requirements are asked of the employer when involved in employee monitoring and in most instances the exceptions provided in the legislation allows employers to conduct business as they wish. Also it is difficult to establish the tort that would warrant a judgement in favor of the employee. Because of it subjective nature, the establishment of this tort is left to a wide range of interpretation. The exceptions in the laws, the difficulty in establishing tort, and the foundation built by these precedents lay the balance of power in the hands of the employer.

CONCLUSION

The employee should acknowledge the fact that the realm of electronic communications is in it developmental stages. The issues and concerns arising from this new technology are new and have not been fully addressed. As a result of this many disputes and claims have arisen that lack sound precedent. Because of the rise in popularity of email, we should expect to see many more laws and cases resembling the ones that I have discussed. In the meantime, employees should expect to receive no privacy if communicating over a corporate network and the substance of their transmissions should retain a professional temperament. Until we can get more defined boundaries the conflict between employees and employers regarding email privacy will rage on.

Jim Kates is a computer consultant specializing in the security design, implementation and audit of client server environments. As a security expert for the past 15 years, he has worked with large businesses and government agencies across the globe. He has consulted worldwide to major financial, manufacturing, aerospace and insurance corporations in the areas of computer security, telecommunication controls, trade secret protection and audit concerns. He coordinates and manages investigations for a large law firm; including investigating product counterfeiting, employee fraud and corporate counterespionage.