December 1999

Ethics and Technology in the Workplace

Yvette McManus

Stephen F. Austin State University

Follow this and additional works at: http://aisel.aisnet.org/amcis1999

Recommended Citation

http://aisel.aisnet.org/amcis1999/223
What is “Business Ethics”? Dr. Carter McNamara, Ph.D. author of the “Complete Guide to Ethics Management: An Ethics Toolkit for Managers” says that it means differentiating between right and wrong in the workplace, and doing what is right. Today’s world offers such a complexity of issues and dilemmas to the employer and the employee, that ethical standards that have long been upheld are now being questioned. With the advent of computers and new technologies, the fundamental workplace rules are changing (McNamara 3).

“New Technologies have changed the way we do our jobs and the way we work with one another,” said Edward Petry, executive director of Ethics Officer Association (EOA), Belmont, Massachusetts. “This increases the risk of unethical and illegal actions” (Dries 1).

This report introduces readers, perhaps college students new to business ethics or to the vast number of questions being raised about technological ethics, to varying aspects of these ethical definitions, functions, approaches, and case studies in the field of electronic communication in the workplace, so that they, as users, become aware of potential, problematical situations in current and future employment.

There are vast areas of misinformation and non-information in the faintly nebulous world of workplace technological ethics. The research I have done indicates that there are many people, employees and employers alike, who do not know the boundaries of their workplace responsibilities and liabilities. This lack sets the stage for the misinterpretation and misuse of the business’s ethics codes. This author attempts to clarify a few of these misconceptions.

Statistics

The following statistics provide a glimpse into the future of techno ethics as we see the rising numbers of companies and businesses using some form of employee surveillance and the disparity among workers’ beliefs concerning what is private and what is not.

“E-Mail is in use, in some capacity, in all Fortune 1000 companies, and it is expected that by the year 2000, 40 million e-mail users will be sending 60 billion e-mail messages a year” (Miller 1).

According to a 1995 survey of human resource professionals, “36 percent of organizations that provide email look at their employees’ email records for business necessity or security; 8 percent conduct random reviews of the email; …75 percent responded that employers should have the right to read company-provided email” (Stellin WHO 1).

In a 1993 MACWORLD survey, researchers found that “E-mail monitoring was done by 42 percent of the companies”.

“Forty-five percent of workers say they have committed at least one of a dozen actions over the past year that are either unethical or fall into a gray area, according to the survey of 726 workers. The survey was sponsored by the American Society of Chartered Life Underwriters & Chartered Financial Consultants and the Ethics Officer Association” (Jones 1).

Techno privacy issues in the business world are constantly increasing as more and more companies utilize some form of employee surveillance, yet 29% of the employees surveyed continue to view company e-mail as being available for personal use.

Law: What Do the Courts Say?

The 1986 Electronic Communications Privacy Act (ECPA) added electronic communications to an earlier bill that restricted the rights of law enforcement agencies to access telephone and wire messages. The problem is that the bill came with a built-in exception; employers (providers of the service) do have the right to monitor e-mail, computer files and other company provided communication systems, even when a company has issued a policy stating that it would not access its employees’ e-mail.

Popular opinion holds that these rights to privacy are protected under the Fourth Amendment, which protects U.S. citizens against unlawful search and seizure by the government; however, according to the ECPA, this does not include the government or private employers. Most states uphold the employer’s right to intercept e-mail – “and even to dismiss an employee based on the content of e-mail messages” (Stellin What 2).

Electronic communications can be used as evidence in a court of law. New federal rules were adopted in December, 1997, that allow the inclusion of e-mail and other electronic data on the list of items that a party must disclose during the pre-trial process called discovery. Asking for e-mail is no different than asking for memos, files or other correspondence.
In her cover story for “INFORMATION WEEK”, Stephanie Stahl gives an example of the use of confiscated e-mail in a high-profile court case:

Former Reagan White House aide Oliver North had his testimony on the Iran-Contra affair challenged when congressional investigators uncovered thousands of E-mail messages that North thought had been deleted (12).

Attorneys say that they feel like they have struck gold when they recover e-mail or files thought to be nonexistent. Juries can see the hard evidence and remember it; it is tangible proof.

Surveillance: Who is Watching, How & Why

Digital technology enables managers and employers to monitor, record and examine e-mail, listen in on telephone conversations, track Internet use in the office and the number of keystrokes the employee makes in a specific time period, and even to track the employee’s activities in the building with the use of a device called an active badge, developed by Olivetti and Xerox.

An astute network manager can eavesdrop on virtually every aspect of a networked computing environment, and can view the contents of data files and electronic mail messages overwrite private passwords, and audit the time and activities an employee spends on the network. One survey indicates that monitoring employee performance by means of computer, telephone or video, is used in 75 percent of organizations.

Although approximately 30 percent of companies with 1000 or more employees engage in some type of monitoring, only 18 percent of these companies actually have ethics monitoring policies in place, and the majority of their employees do not realize any surveillance is in use.

Most network management programs within companies can be set up to keep copies of inbound and outbound messages. Software developers can and do easily provide businesses with software designed to use certain key words such as: sex, job search, employment and resume to spark a response and tag a message you thought was private. Even if your network is not programmed to automatically copy all e-mail, it is probably set to make regular backups of computer material, so that when the network gets backed up, your mail gets copied, too. Susan Stellin’s description, in her article “What do the Courts Say?”, about the Alana Shoars case exemplifies the law’s attitude toward companies backing up email:

“Probably the best-known case involving email privacy is Flanagan et al. Vs. Epson America, Inc. In this case, Epson employee Alana Shoars found printouts of all the email messages that had been sent to or from the company’s Torrance, California, facility during a two-month period in 1989. Shoars filed a class-action suit on behalf of herself and other employees, claiming invasion of privacy (under California’s constitution and a wiretapping statute). The state court ruled against Shoars on the grounds that email was not covered by California’s wiretapping statute and that the right to privacy guaranteed by the state constitution covered personal but not business information.”

Misuse of the Internet and e-mail is one of the major reasons employers give for monitoring their employees. Although the World Wide Web is the source for much new business and provides many new benefits, employers show concern over the possibility that employees will spend company time with personal business or entertainment. Susan Stellin, in her article “Why all the Snooping” for CNET Special Reports says, “A study released on April 2 by Network World magazine found that 70 percent of executives surveyed believe their employees use the Net for entertainment on company time” (1).

The fear of lawsuits is very real in the corporate world. Some employers maintain that monitoring e-mail is one way to discover and prevent workplace abuse such as harassment while it can still be contained. Monitoring is a means of discovering whether or not employees are sending messages with sexist or racial overtones. With the use of some form of surveillance, those issues could be addressed and curtailed without suffering legal repercussions throughout the company.

Data Recovery

Many computer users are under the false impression that once they have deleted a message or file it disappears as if it never existed. This is an illusion, a false sense of security. Today, there are many programs available for the retrieval of messages that are assumed lost in Cyberspace.

Users do not stop to consider that with one stroke of the “Send” key, a single message sent to just one person can be forwarded to hundreds and thousands of others. The best rule-of-thumb is: if you would not shout your message to the world, don’t send it via e-mail. There are plenty of electronic detectives waiting to find your message and use it against you.
Privacy in electronic communication has many aspects. We have examined the legal aspect, the surveillance aspect and the recovery aspect of what is becoming an issue fraught with loopholes and frightening language to the uninitiated. What are the psychological effects of privacy in the workplace?

Workers who can maintain a sense of self-worth and a feeling of control while employed are more likely to produce more in a shorter period with greater company loyalty. If the employer has notified the employees that their e-mail will be monitored, told them the restrictions and provided guidelines, the privacy issue will be diffused before growing into a monster to be challenged.

“Recent studies have shown that monitored employees report higher instances of tension, anxiety, depression, anger and frustration than non-monitored workers” (Smith 230-1).

Policy Suggestions

Many companies are appointing on-site committees to examine privacy issues and to formulate balanced policies that adhere to the security needs within the business, but also to strike a balance with the individual’s need to feel trusted. The diversity of e-mail ethics policies reflects the diversity of business interests in the corporate world.

Borland’s e-mail policy states that they reserve the right to conduct a routine inspection or search for Borland property at any time. They don’t look at e-mail to evaluate employees unless there’s a unique situation.

“When Borland’s Eugene Wang left the company to work for Symantec Corporation in 1993, Borland seized his data on both the company machine and his home machine. Borland charged that before leaving, Wang had revealed top-secret corporate data, including marketing plans, and product-release dates to Symantec, a direct competitor. Wang claimed that the data was utilized on a private network; Borland countered that they paid for Wang’s MCI mail account. This case is one of many that set new legislative standards for computer and e-mail monitoring” (Smith, Hanebury 229).

Texas Instruments provides information on a business-card size mini-pamphlet to carry at all times. “Is the action legal? Does it comply with our values? If you do it, will you feel bad? How will it look in the newspaper? If you know its wrong, don’t do it! If you’re not sure, ask! Keep asking until you get an answer” (T.I.).

Each company, regardless of size, needs to protect its employees and itself with a definitive privacy policy. This action would eliminate many problems that arise because of a lack of information and instruction.

Survey Responses – What do Employees Think?

There are many gray areas remaining in the field of e-mail privacy law, and the employee in today’s workplace must tread a fine line when deciding what to put into writing over the electronic mediums. Listed are a couple of the comments by employees about their general feelings on this issue. (To protect their individual privacy, names are not used.)

“…Information is a corporate commodity. The desk where I work, the phone I use, the computer time I spend; these are all corporate assets. They belong to the company, not to me, and that includes my e-mail ID. It may not be “nice” that managers can monitor employees’ work, search their desks, read their e-mail, but face; they can.”

“It is my responsibility to think long and hard about what information I want to transmit, rather than complain that it ended up in the wrong hands.”

The techno-ethics issue is as diverse as the population of employees and employers. Information is the best solution to the diversity.

What Do You Think?

Where do you stand on the employees’ rights? In the world of techno-ethics, there are few mandated rules and many areas where it is left to each individual employer to decide what ethical rules to impose on employees. Although many employees disagree with what they consider an infringement of their right to privacy, the pace is accelerating toward more employer control and more government control. In many cases, the control and monitoring is justified by the need for business security and even by the loosely held ethical views of the employees, but is this control getting out of hand?

If you find it difficult to answer these questions, take comfort in knowing that you are one among many who are attempting to make sense of and find answers to the confusing maelstrom of Ethics and Technology in the Workplace.

References available upon request from Yvette McManus.