Complete Annotated MLA Research Paper

Your last name and the page number should appear in a header on each page, upper right corner. Double-space the entire paper and Works Cited page.

Hal Stevens
Professor Daniels
BUS 321
24 May 2013

Using Work Computers for Personal Business is Not a Problem

This introductory paragraph serves as a hook to grab the reader's attention and to increase interest in the writer's situation.

A familiar scene plays out in offices everywhere. An employee sitting in his cubicle has just finished a project, grabbed a cup of coffee, and is taking a 15-minute break. He pulls up the Ohio State Buckeyes web site to scout next season's potential recruits. Then he plays a game or two of computer Solitaire. A quick check on his personal email account to see if the birthday present he ordered for his wife has been shipped from Sears yet. Break over, the employee returns to his next project. A week later, he is surprised and angered to be called to his supervisor's office and subjected to a reprimand. The subject? Misusing the company's computers. What employees regard as private computer use during personal time turns out to be not so private after all.

In the above scenario, the company has installed new computer surveillance software, which now monitors employees' every keystroke, visits to online sites, and emails—personal or work-related. Is this an invasion of privacy? Is it legal? The answer is a complicated "yes" and "no." Certain kinds of situations are covered by the topic of privacy, others by the legality of the surveillance performed and whether employees are notified of company monitoring policies. Mostly, though, business owners are able to monitor employee computer use at will. Although it is reasonable that companies expect their employees to use company computers for company activity, it is also understandable and desirable that employees have privacy rights at work in regards to their computer usage.

Here, after a question, Hal states his claim.

France Bélanger and Robert E. Crossler, researchers in the field of information privacy and security, find that little existing research focuses on the issue of electronic privacy of personal information in the workplace. They cite a Pew Internet Project survey, however, that indicates 85% of adults find it of the utmost importance to protect their personal information (1017).

The Electronic Privacy Information Center (EPIC) is a clearinghouse that gathers information on workplace privacy. A recent article, "Workplace Privacy," lists the most frequent types of workplace monitoring:

- Phone monitoring
- Video surveillance
- ID tags that can monitor an employee's location (including GPS monitors that can track employees on the road)
- Keystroke loggers
- Email and Internet usage

In an interview I conducted with Gary Hopkins, CEO of Farm Fresh, an Organic Foods wholesale, he indicates that most of his employees do not like their work habits being subjected to monitoring, but there is little that they can do to prevent it. Hopkins says keeping workers on notice with email and Internet monitoring has increased productivity 22% in the last year alone.

Currently there are few laws that cover the ever-changing technology of electronic communications, as Nancy Flynn, author of the *e-Policy Handbook*, explains:

> In the United States and many third-world countries, workers have very few privacy protections in law. There are few situations where an employee has a due process right to access, inspect, or challenge information collected or held by the employer. There are a patchwork of state and federal laws that

This paragraph gives background material on the subject of electronic monitoring practices. Some background is usually needed to explain the situation that has led to the controversy about an issue.

Introduction of a long quote that is set off 10 spaces from the margin. If the author had not been introduced before the quotation (as is the case here), the citation would appear at the end of the quote, AFTER the period.

Complete Annotated MLA Research Paper

> grant employees limited rights. For instance, under federal law, private-sector employees cannot be required to submit to a polygraph examination. However, there are no general protections of workplace privacy except where an employer acts tortuously—where the employer violates the employee's reasonable expectation of privacy.

One law that would seem to be on the side of employees' privacy is the 1986 United States Electronic Privacy Act (ECPA), which "prohibits reading or disclosure of the contents of any electronic communication not intended for the reader" (Teel 6). One important exemption from this act, however, is an employer who owns a company's email system. Several court cases have also sided with employers.

Lothar Determann and Robert Sprague's article comparing advances in European workplace privacy with the lacks in American privacy, points out that in the United States, people have a constitutional expectation of privacy in general, but a low expectation of privacy in the workplace (1022).

Determann and Sprague also explain that employer monitoring has been able to extend its scope to scan emails for viruses and spam and other links that may be harmful to the employees' computers in particular, but to the company network in general. In scanning for harmful activity, workers' log-ons, emails, screen activity, web site visits, among other types of information can be accessed (982). Uncomfortable for employees, though, are the monitoring possibilities that extend beyond company security to track Internet access, electronic chats and online sessions, and remote viewing that may not be work-related. Another concern is that with GPS and wireless features, employees who work from home can be monitored as well (982).

For example, in *Smyth vs. The Pillsbury Company* (1994), Michael Smyth was fired from his job for sending "inappropriate and unprofessional" comments from his home computer using Pillsbury's email system. The comments to his supervisor "contained threats to 'kill the backstabbing bastards' and referred to the planned Holiday party as the 'Jim Jones Koolaid affair.'" Smyth argued that he had a "reasonable expectation of privacy" in sending emails, regardless of content, because Pillsbury's policies on emails was that they would not be monitored or read. The Pennsylvania District Court ruled in favor of the employer saying, "the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments."

This example is long enough that it warrants its own paragraph. Resist the temptation to cram as much as you can in one paragraph just because it is all on the same topic.

In addition to problems associated with sending email, there are also concerns about employees spending their work time surfing the Internet or playing computer games. North Carolina State Senator Austin Allran, for example, believes that the government would save millions of dollars now currently lost to state and federal employees playing Solitaire on their office computers if the games were removed from employees' computers (Johnsson).

A topic sentence introducing support.

New York City mayor Michael Bloomberg even fired an employee when he saw an in-progress game on the employee's computer. The employee admitted to occasionally playing a game to take a break from exhausting work, but Bloomberg believes that no time should be spent playing computer games during work time ("Employee Monitoring"). Patrik Johnsson notes that the suggested removal of games like Solitaire from worker's computers "goes straight to the issue of distractions from long days at the office and, more fundamentally, how much of their employees' time and concentration employers can reasonably expect to own."

Some proponents of leaving the games on workers' computers argue that they actually increase employee productivity by providing an outlet for stress relief ("Employee Monitoring"). So although many employees who spend a lot of time staring at computer screens feel that taking a break with a computer game rejuvenates them, employers see the time spent "rejuvenating" as wasteful.

But a far more serious problem is employees using the company's Internet connection to access inappropriate web sites. Some employees will visit sites at work that they may not want those they live with to know about, for example pornographic sites, or ones that deal with alternative lifestyles, violence, or drugs.

A total of 304 companies participated in the 2007 Electronic Monitoring and Surveillance Survey sponsored by both the American Management Association and the ePolicy Institute. Here are the results of several of the questions about company Internet usage:

- 83% of the respondents said that their organization has a written policy governing the personal use of the Internet.
- 16% of employers record phone conversations; 84% notify employees that their phone conversations are monitored, but only 73% notify employees that their voicemails are also monitored.
- 65% of companies use software to block inappropriate sites (social networking, pornographic, and entertainments sites top the list).

The survey also indicates that although companies have policies regarding electronic privacy, employees rarely read or otherwise pay attention to the policies.

Another topic sentence introducing support. Notice that the items of support seem to be presented in increasingly important order.

Complete Annotated MLA Research Paper

Most employees would likely agree that visiting certain sites or spending a *significant* amount of time surfing the Internet for non job-related information canbe a problem. But what about smaller increments of time that might act as productive breaks? If any email system provided by an employer is subject to monitoring, how much privacy are employees really allowed at work?

Employers assert that they have a right to know what their employees are doing on company time, particularly with company computers and email systems. Companies worry about loss of productivity. Nancy Flynn notes that employer termination for email and web misuse is increasing: employer terminations for email violations, ranging from violation of company policies and excessive personal use, rose from 14% in 2001 to 28% in 2007 (182). But for employees who spend enormous numbers of hours at work, using email is one of the best ways to take care of personal business that cannot be done after work, such as making doctors' appointments.

Companies also worry about employees giving competitors access to trade secrets and about charges of allowing a hostile work environment if harassing emails are sent from an office computer (Dell and Kullen). Courts mostly side with companies, although occasionally a defendant wins. In *United States vs. Slanina*, the Fifth Circuit Court of Appeals found that because the company by whom Slanina was employed did not have a posted policy about computer usage or Internet monitoring, he "had a reasonable expectation of privacy in his office computer" (Cassily and Draper).

It is the issue of reasonable expectations of privacy which poses the largest stumbling block for a solution to workplace privacy issues. What seems

An item of qualification. Employees do realize that surfing while working can be a waste of time, but they may question the need for oversight of all activity.

Items of opposition. What are some opposing views? How can they be addressed?

Complete Annotated MLA Research Paper

reasonable to a boss may not seem reasonable to employees. In 1993, Congress passed the Privacy for Consumers and Workers Act. This piece of legislation doesn't ban electronic monitoring, but states that employees must be given notice that they are subject to monitoring in the workplace (Rich). But how does this work for telecommuting employees? Some of the privacy issues that have not been resolved in the area of monitoring employees who work from home are

- the difficulty of the employer to monitor an employee's work at home without crossing over into the employee's private life,
- the inability to determine when an employee is on "duty,"
- and the inability to differentiate between an employee using the computer and another family member. ("Workplace Privacy")

As technology advances, new issues involving the rights of employees to maintain privacy of their electronic lives (email, Internet usage, etc.) will become more tangled. How far can an employer go in scrutinizing their employee's emails? Addressing employees' reasonable expectations of privacy and notifying them of workplace policies are practices already in place for many businesses, but there is no law forcing private businesses to follow these guidelines. The Fourth Amendment guarantees the right of citizens to be safe from unreasonable searches of their "persons, houses, papers and effects" by the government. However, the Internet was not even a faint glimmer of possibility in 18th century America. Should we add an amendment to the Bill of Rights covering electronic privacy? Maybe that is coming.

Hal's conclusion rounds out the discussion, adding interesting material for the reader to think about without offering new items of support or changes of direction.

Works Cited

American Management Association. "2007 Electronic Monitoring & Surveillance Survey: Many Companies Monitoring, Recording, Videotaping—and Firing—Employees." *AMA*. American Management Association, 2008. Web. 21 May 2013.

Bélanger, France, and Robert E. Crossler. "Privacy in The Digital Age: A Review of Information Privacy Research in Information Systems." *MIS Quarterly* 35.4 (2011): 1017-A36. *Business Source Premier*. Web. 21 May 2013.

Casilly, Lisa H., and Clare H. Draper. *Workplace Privacy: A Guide for Attorneys and HR Professionals*. Boston: Pike and Fischer, 2004. Print.

Dell, Kristina, and Lisa Takeuchi Kullen. "Snooping Bosses." *Time* 11 Sept. 2006: 62–64. *EBSCOhost*. Web. 21 May 2013.

Determann, Lothar, and Robert Sprague. "Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States." *Berkeley Technology Law Journal* 26 (2011): 979–1036. Web. 21 May 2013.

"Employee Monitoring: Is There Privacy in the Workplace?" *Privacy Rights Clearinghouse*. Privacy Rights Clearinghouse, Feb. 2006. Web. 21 May 2013.

Flynn, Nancy. *e-Policy Handbook*. 2nd ed. New York: AMACOM, 2009.

Hopkins, Gary. Personal Interview. 13 May 2013.

Johnsson, Patrik. "Is That a Spreadsheet on Your Screen or Solitaire?" *CSMonitor.com*. The Christian Science Monitor, 18 Mar. 2005. Web. 30 Mar., 2013.

Rich, Lloyd L. "Right to Privacy in the Information Age." *Publishing Law Center*. Publishing Law Center,1995. Web. 21 May 2013.

"Smyth vs. The Pillsbury Company (1994)." *Privacy in Cyberspace*. Harvard Law School, n.d. Web. 30 May 2013.

Teel, Linda M. "Confidentiality and Electronic Mail: Issue of Privacy." *Delta Kappa Gamma Bulletin* 72.4 (2006): 5-8. *EBSCOhost*. Web. 21 May 2013.

"Workplace Privacy." *EPIC*. Electronic Privacy Information Center, 25 July 2006. Web. 21 May 2013.

Creating Print Version