MLA Research Paper (Orlov)

Anna Orlov
Professor Willis
English 101
17 March XXXX

Title is centered.

Online Monitoring:

A Threat to Employee Privacy in the Wired Workplace

Opening sentences provide background for thesis.

As the Internet has become an integral tool of businesses, company policies on Internet usage have become as common as policies regarding vacation days or sexual harassment. A 2005 study by the American Management Association and ePolicy Institute found that 76% of companies monitor employees' use of the Web, and the number of companies that block employees' access to certain Web sites has increased 27% since 2001 (1). Unlike other company rules, however, Internet usage policies often include language authorizing companies to secretly monitor their employees, a practice that raises questions about rights in the workplace. Although companies often have legitimate concerns that lead them to monitor employees' Internet usage--from expensive security breaches to reduced productivity--the benefits of electronic surveillance are outweighed by its costs to employees' privacy and autonomy.

Thesis asserts Orlov's main point.

Summary and long quotation are introduced with a signal phrase naming the author.

While surveillance of employees is not a new phenomenon, electronic surveillance allows employers to monitor workers with unprecedented efficiency. In his book The Naked Employee, Frederick Lane describes offline ways in which employers have been permitted to intrude on employees' privacy for decades, such as drug testing, background checks, psychological exams, lie detector

Marginal annotations indicate MLA-style formatting and effective writing.

Source: Diana Hacker (Boston: Bedford/St. Martin's, 2007).

tests, and in-store video surveillance. The difference, Lane argues, between these old methods of data gathering and electronic surveillance involves quantity:

> Technology makes it possible for employers to gather enormous amounts of data about employees, often far beyond what is necessary to satisfy safety or productivity concerns. And the trends that drive technology--faster, smaller, cheaper--make it possible for larger and larger numbers of employers to gather ever-greater amounts of personal data. (3-4)

Long quotation is set off from the text; quotation marks are omitted.

Page number is given in parentheses after the final period.

Lane points out that employers can collect data whenever employees use their computers--for example, when they send e-mail, surf the Web, or even arrive at or depart from their workstations.

Another key difference between traditional surveillance and electronic surveillance is that employers can monitor workers' computer use secretly. One popular monitoring method is keystroke logging, which is done by means of an undetectable program on employees' computers. The Web site of a vendor for Spector Pro, a popular keystroke logging program, explains that the software can be installed to operate in "Stealth" mode so that it "does not show up as an icon, does not appear in the Windows system tray, . . . [and] cannot be uninstalled without the Spector Pro password which YOU specify" ("Automatically"). As Lane explains, these programs record every key entered into the computer in hidden directories that can later be accessed or uploaded by supervisors; at their most sophisticated, the programs can even scan for keywords tailored to individual companies (128-29).

Clear topic sentences, like this one, are used throughout the paper.

Source with an unknown author is cited by a shortened title.

Source: Diana Hacker (Boston: Bedford/St. Martin's, 2007).

Orlov anticipates objections and provides sources for opposing views.

Some experts have argued that a range of legitimate concerns justifies employer monitoring of employee Internet usage. As PC World columnist Daniel Tynan explains, companies that don't monitor network traffic can be penalized for their ignorance: "Employees could accidentally (or deliberately) spill confidential information . . . or allow worms to spread throughout a corporate network." The ePolicy Institute, an organization that advises companies about reducing risks from technology, reported that breaches in computer security cost institutions $100 million in 1999 alone (Flynn). Companies also are held legally accountable for many of the transactions conducted on their networks and with their technology. Legal scholar Jay Kesan points out that the law holds employers liable for employees' actions such as violations of copyright laws, the distribution of offensive or graphic sexual material, and illegal disclosure of confidential information (312).

Transition helps readers move from one paragraph to the next.

These kinds of concerns should give employers, in certain instances, the right to monitor employee behavior. But employers rushing to adopt surveillance programs might not be adequately weighing the effect such programs can have on employee morale.

Employers must consider the possibility that employees will perceive surveillance as a breach of trust that can make them feel like disobedient children, not responsible adults who wish to perform their jobs professionally and autonomously.

Orlov treats both sides fairly; she provides a transition to her own argument.

Yet determining how much autonomy workers should be given is complicated by the ambiguous nature of productivity in the wired workplace. On the one hand, computers and Internet access give employees powerful tools to carry out their jobs; on the other

Source: Diana Hacker (Boston: Bedford/St. Martin's, 2007).

Fig. 1. Scott Adams, Dilbert and the Way of the Weasel (New York: Harper, 2002) 106.

Illustration has figure number and source information.

hand, the same technology offers constant temptations to avoid work. As a 2005 study by Salary.com and America Online indicates, the Internet ranked as the top choice among employees for ways of wasting time on the job; it beat talking with co-workers--the second most popular method--by a margin of nearly two to one (Frauenheim). Chris Gonsalves, an editor for eWeek.com, argues that the technology has changed the terms between employers and employees: "While bosses can easily detect and interrupt water-cooler chatter," he writes, "the employee who is shopping at Lands' End or IMing with fellow fantasy baseball managers may actually appear to be working." The gap between behaviors that are observable to managers and the employee's actual activities when sitting behind a computer has created additional motivations for employers to invest in surveillance programs. "Dilbert," a popular cartoon that spoofs office culture, aptly captures how rampant recreational Internet use has become in the workplace (see Fig. 1).

No page number is available for this Web source.

But monitoring online activities can have the unintended effect of making employees resentful. As many workers would be quick to point out, Web surfing and other personal uses of the

Orlov counters opposing views and provides support for her argument.

Source: Diana Hacker (Boston: Bedford/St. Martin's, 2007).

Internet can provide needed outlets in the stressful work environment; many scholars have argued that limiting and policing these outlets can exacerbate tensions between employees and managers. Kesan warns that "prohibiting personal use can seem extremely arbitrary and can seriously harm morale. . . . Imagine a concerned parent who is prohibited from checking on a sick child by a draconian company policy" (315-16). As this analysis indicates, employees can become disgruntled when Internet usage policies are enforced to their full extent.

Orlov uses a brief signal phrase to move from her argument to the words of a source.

Additionally, many experts disagree with employers' assumption that online monitoring can increase productivity. Employment law attorney Joseph Schmitt argues that, particularly for employees who are paid a salary rather than by the hour, "a company shouldn't care whether employees spend one or 10 hours on the Internet as long as they are getting their jobs done--and provided that they are not accessing inappropriate sites" (qtd. in Verespej). Other experts even argue that time spent on personal Internet browsing can actually be productive for companies. According to Bill Coleman, an executive at Salary.com, "Personal Internet use and casual office conversations often turn into new business ideas or suggestions for gaining operating efficiencies" (qtd. in Frauenheim). Employers, in other words, may benefit from showing more faith in their employees' ability to exercise their autonomy.

Orlov cites an indirect source: words quoted in another source.

Employees' right to privacy and autonomy in the workplace, however, remains a murky area of the law. Although evaluating where to draw the line between employee rights and employer

Source: Diana Hacker (Boston: Bedford/St. Martin's, 2007).

powers is often a duty that falls to the judicial system, the courts have shown little willingness to intrude on employers' exercise of control over their computer networks. Federal law provides few guidelines related to online monitoring of employees, and only Connecticut and Delaware require companies to disclose this type of surveillance to employees (Tam et al.). "It is unlikely that we will see a legally guaranteed zone of privacy in the American workplace," predicts Kesan (293). This reality leaves employees and employers to sort the potential risks and benefits of technology in contract agreements and terms of employment. With continuing advances in technology, protecting both employers and employees will require greater awareness of these programs, better disclosure to employees, and a more public discussion about what types of protections are necessary to guard individual freedoms in the wired workplace.

Orlov sums up her argument and suggests a course of action.

Source: Diana Hacker (Boston: Bedford/St. Martin's, 2007).

Heading is centered.

Works Cited

List is alphabetized by authors' last names (or by title when a work has no author).

Adams, Scott. Dilbert and the Way of the Weasel. New York: Harper, 2002.

American Management Association and ePolicy Institute. "2005 Electronic Monitoring and Surveillance Survey." American Management Association. 2005. 15 Feb. 2006 <http://www.amanet.org/research/pdfs/EMS_summary05.pdf>.

"Automatically Record Everything They Do Online! Spector Pro 5.0 FAQ's." Netbus.org. SpectorSoft. 17 Feb. 2006 <http://www.netbus.org/sProFAQ.html>.

Flynn, Nancy. "Internet Policies." ePolicy Institute. 2001. 15 Feb. 2006 <http://www.epolicyinstitute.com/i_policies/index.html>.

Frauenheim, Ed. "Stop Reading This Headline and Get Back to Work." CNET News.com. 11 July 2005. 17 Feb. 2006 <http://news.com.com/Stop+reading+this+headline+and+get+back+to+work/2100-1022_3-5783552.html>.

Gonsalves, Chris. "Wasting Away on the Web." eWeek.com 8 Aug. 2005. 16 Feb. 2006 <http://www.eweek.com/article2/0,1895,1843242,00.asp>.

Kesan, Jay P. "Cyber-Working or Cyber-Shirking? A First Principles Examination of Electronic Privacy in the Workplace." Florida Law Review 54 (2002): 289-332.

Lane, Frederick S., III. The Naked Employee: How Technology Is Compromising Workplace Privacy. New York: Amer. Management Assn., 2003.

The URL is broken after a slash. No hyphen is inserted.

First line of each entry is at the left margin; extra lines are indented ½" (or five spaces).

Double-spacing is used throughout.

Source: Diana Hacker (Boston: Bedford/St. Martin's, 2007).

Tam, Pui-Wing, et al. "Snooping E-Mail by Software Is Now a Workplace Norm." Wall Street Journal 9 Mar. 2005: B1+.

Tynan, Daniel. "Your Boss Is Watching." PC World 6 Oct. 2004. 17 Feb. 2006 <http://www.pcworld.com/news/article/0,aid,118072,00.asp>.

Verespej, Michael A. "Inappropriate Internet Surfing." Industry Week 7 Feb. 2000. 16 Feb. 2006 <http://www.industryweek.com/ReadArticle.aspx?ArticleID=568>.

A work with four authors is listed by the first author's name and the abbreviation "et al." (for "and others").

Source: Diana Hacker (Boston: Bedford/St. Martin's, 2007).