# CSE 303, Autumn 2008, Sample Paper

*This is merely one example for an assignment that is quite broad.*

Article discussed:
G. Daryl Nord, Tipton F. McCubbins, and Jeretta Horn Nord. E-monitoring in the workplace: privacy, legislation, and surveillance software. *Communications of the ACM*, 49(8): 72–77, 2006.
Available at `http://doi.acm.org/10.1145/1145287.1145290`

E-Monitoring Article Raises Important Examples but Ignores the Role of Disclosure

Workplace electronic monitoring, in which employers track computer activity and data of employees, is a difficult ethical issue because it must balance the needs of the organization with the privacy of its members. As the article by Nord et al explains, technology is already available that allows very intrusive monitoring, such as real-time data describing each user's keystrokes and screen content. There are also relevant United States laws and court decisions that largely support employers' use of employee computer activity, even of email kept in a password-protected and encrypted folder. This summary of technological capabilities and laws is very useful, as is a discussion of the reasons organizations have for electronic monitoring. However, the article does a poor job of discussing what obligations organizations have to disclose their monitoring policies and inform employees.

Though the article does not present it this way, we can classify monitoring activities into those tracking current activity and those that store data for monitoring later. A tool that lets a system administrator silently view any instant-messaging conversation is in the former category, and an archive of all email sent and received in the latter. Both forms raise troubling privacy concerns. The former can make it impossible for an employee to do the electronic equivalent of "closing the door" for a moment of privacy. The latter can make it impossible for an employee to get rid of embarrassing or personal information as soon as it (perhaps accidentally) "touches" a corporate computer. It also increases the chance the data could be stolen or used for a purpose never considered when an employee created the data.

However, the article raises several legitimate reasons and legal justifications for electronic monitoring. First, network monitoring is important for ensuring limited resources (such as network bandwidth) are used efficiently. Second, network security can make it important to ensure employees do not download viruses. Third, protecting company secrets can justify screening all outgoing data. Fourth, organizations need to enforce workplace laws and policies such as preventing harassment. Fifth, monitoring can ensure employee productivity.

While the focus of the article is what organizations may legally monitor, an equally important consideration is how employees can be informed about monitoring in an understandable and balanced way. If every second of computer use by an employee will be recorded, retained forever, and made available to anyone in the company, then at the very least employees should

know that. Perhaps different applications could have easy-to-notice flags in the graphical user-interface such as, "recorded," "monitored live," or "private." Also not discussed in the article is what right employees have to learn what is being monitored and archived. Is there some legal mechanism by which employees can see the recorded information just like they have certain rights to see their personnel file?

As the article mentions briefly, there is legally protected privacy in the workplace, such as a locker provided to an employee with a lock for which only the employee has the key. While court cases have decided that computer files like email folders are not equivalent to personal lockers, there is no discussion of whether we *need* some sort of equivalent in a world where so much of one's valuable property is digital. For example, presumably the data on a personal cell phone or disk drive in an employee's pocket is private, but can an employer worried about security prohibit employees from bringing such devices to work?

In general, computers in the workplace have had the unintended consequence of monitoring and recording much more of an employee's activity than in the past. There are legitimate reasons for monitoring an employee's computer activity, but there are also legitimate reasons for employees to do something private. This article focused on what monitoring is legal but did not give employees much guidance on what they can do to learn what is monitored or what alternatives they might have.