

UNIVERSITY OF WATERLOO  
FACULTY OF MATHEMATICS  
DEPARTMENT OF COMPUTER SCIENCE

# CS 492: Assignment 3

Darik Horn, 00000000  
For Professor Robin Cohen, Section 01  
2002/02/05

## Contents

1.0 Electronic Monitoring	2
1.1 Legacy Monitoring Technologies	2
1.2 Computer Monitoring Technologies	2
1.3 Technology Summary	2
2.0 Applications of Electronic Monitoring	3
2.1 Legality	3
2.2 Data Archiving	3
2.3 Control and Security	3
2.4 Legal Pressure	4
2.5 Market Penetration	4
2.6 Application Summary	4
3.0 Employee Impact of Electronic Monitoring	5
3.1 Privacy	5
3.2 Social Consequences	5
4.0 Balancing Interests	6
4.1 Ashby's Law of Requisite Variety	6
4.2 Perrow's Job Class Typology	6
5.0 Conclusion	7

## 1.0 Electronic Monitoring

Electronic monitoring is the activity of using automated devices to intercept communications and record activity.

### 1.1 Legacy Electronic Monitoring Technologies

Sound and video surveillance technologies are mature and have been available as commodity products for many years. Companies like Bolide Corporation mass-produce office appliances that contain hidden wireless cameras and microphones.

A corporation may affordably deploy covert monitoring devices in smoke alarms, desk radios, fire-exit signs, pens, telephones, and briefcases<sup>1</sup>. A company may, alternatively, use more conventional devices like wall-mounted closed-circuit television cameras and punch-clocks.

### 1.2 Computer Electronic Monitoring Technologies

There exist technologies to tap the flow of information between the user and the computer. Monitoring software for most computing platforms is readily available. On Unix platforms, programs like 'ttsnoop' are often bundled with the operating system, whereas numerous commercial turnkey monitoring solutions are available for Microsoft platforms.<sup>2</sup>

Computer monitoring has the finest granularity among all monitoring technologies. A computer systems administrator may only record the times when a computer user connects to the system, or they may rebroadcast every keystroke and mouse click made by that computer user to a manager's desktop.

### 1.3 Technology Summary

Technology provides corporations with an absolute ability to monitor employee communications and to record employee behavior, entirely without the employee being aware of such activity. Technical feasibility is not an issue, so the only practical limit of electronic monitoring is how much time and money a corporation wishes to spend on implementation.

---

<sup>1</sup> See [http://www.espymall.com/html/Hidden\\_Cameras.html](http://www.espymall.com/html/Hidden_Cameras.html) for hardware examples.

<sup>2</sup> Baltimore MIMesweeper, Websense, SurfControl SuperScout, Symantec I-Gear, Elron Internet Manager, and Tumbleweed MMS are all popular software packages.

## 2.0 Applications of Electronic Monitoring

### 2.1 Legality

In Canada, employee monitoring is legal if the employee is being monitored is notified and if no private information learned about the employee through monitoring is released to third parties.<sup>3</sup>

In the United States of America, all forms of computer monitoring by employers are legal, insofar as employees are notified that they are being monitored.<sup>4</sup>

### 2.2 Data Archiving

Companies will backup and archive computer systems to protect against data loss caused by hardware failure, user mistakes, and intentional vandalism.

Electronic message archives are like the memory of a corporation. Very often, electronic voice and e-mail archives can be used to confirm and verify prior communications between employees, or to search for some company-specific piece of knowledge.

The validity and necessity of data archiving is, for the most part, self-evident.

### 2.3 Control and Security

Corporations have always monitored their employees to maintain internal control. Without an ability to observe and record employee behavior, corporations would be unable to evaluate employee performance. The advent of electronic monitoring has not changed the fundamental basis of this employer-employee relationship, but it has provided managers with a means to garner practically unlimited quantities of data about employee behavior.

However, the large amount of data that electronic monitoring technologies can provide to managers has changed the decision environment of employee evaluations. Managers now have the secondary – and possibly confounding – problem of deriving relevant information from the additional data.

In the same regard, electronic monitoring technologies have provided corporations with tools to better identify the abuse of corporate resources, the theft of corporate property, and the waste of time..

---

<sup>3</sup> The Personal Information Protection and Electronic Documents Act, Bill C6  
[http://www.privcom.gc.ca/legislation/02\\_06\\_01\\_01\\_e.asp](http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp)

<sup>4</sup> The Electronic Monitoring Act; 106th US Congress, 2<sup>nd</sup> Session, Bill 4908  
[http://thomas.loc.gov/cgi-bin/query/z?c106:H.R.4908:](http://thomas.loc.gov/cgi-bin/query/z?c106:H.R.4908)

## 2.4 Legal Pressure

There are many legal pressures for corporations to maintain records of all business activities. The electronic monitoring of employees is an effective due-diligence procedure.

First, if a corporation holds a patent that is challenged by a competitor, then the courts will demand that the corporation produce evidence of research and development. To build a strong case, the corporation would need to submit as many documents and interpersonal messages regarding the patent application as it could find. The patent court would try to determine how the corporation's employees were inspired, and a solid proof of innovation might reveal intimate and personal information about employee thoughts and activities.

Second, corporations can be held liable for the actions of their employees. In order to defend against negligence, harassment, and slander lawsuits, corporations must keep records of employee activity. The corporation would be unable to build a defense if it did not have logs, transcripts, and tapes of employee interaction with the outside world. Under Canadian law, a corporation may be held liable for fostering a hostile workplace if they do not control the web surfing habits of its staff.

Third, governments may impose minimal standards of control upon corporations. The nature of the banking industry, for example, requires that employees be closely watched. No bank customer would ever complain that the people who handle their money are too closely monitored.

## 2.5 Market Penetration

It is estimated that, worldwide, 27% of all employees with network-connected computers are being fully monitored, and that at least half of all employees have their primary channel of communication monitored.<sup>5</sup>

## 2.6 Application Summary

There are no compelling business reasons for corporations not to deploy electronic monitoring technologies. Electronic monitoring technologies are cheap and effective, so there will be a natural tendency for corporations to further expand their application in the workplace.

---

<sup>5</sup> Andrew Schulman; The Extent Of Systematic Monitoring of E-Mail and Internet Use; July 9, 2001.

### 3.0 Employee Impact

#### 3.1 Privacy

Humans are social animals that lack restraint. It is impossible for somebody to fully disconnect and suppress their personal life when they walk into their place of employment. Corporations that electronically monitor their employees will inevitably learn personal details.

Similarly, it is impossible for management to fully separate an employee's private life from their professional life. Management will form attitudes about employees based on the sum-total of their knowledge, regardless of whether the things that they have learned about an employee are all pertinent to the job. If, for example, a manager learns that a female employee is pregnant, they may surreptitiously arrange to terminate that employment relationship.

Furthermore, the corporation has no real financial incentive to keep personal information secure, but also no financial incentive to discard it. The private information learned about employees through electronic monitoring could be stored in a many different computers indefinitely, and accidentally or maliciously released.

#### 3.2 Social Consequences

A culture of surveillance is a culture of distrust. Strong team relationships cannot be formed in environments where people fear communicating because their words may be recorded and used against them in the future.

Electronic monitoring is an affront to personal dignity. A corporation that uses electronic monitoring is tacitly admitting that its employees are untrustworthy. This lack of respect will tend to become mutual, and the emotional gap between staff and management will widen.

Even if a corporation uses electronic monitoring only as a preventative measure, or to positively identify a small group of dishonest people, the realized effect will be that all employees are demoralized by the action.

## 4.0 Balancing Interests

In the context of electronic monitoring, the interests of employers and the interests of employees are contradictory. However, there is an existing and well-accepted business model that can be extended to balance the interests of both parties.

### 4.1 Ashby's Law of Requisite Variety

Ashby's Law of Requisite Variety states that solving a problem of some definite complexity requires using a solution methodology with greater complexity.

In terms of the work environment, this means that employees in high problem variety jobs need more freedom from management to do their work properly, and employees in low problem variety jobs need less freedom from management to do their work properly.

### 4.2 Perrow's Job Class Typology

Perrow subsequently took Ashby's Law crossed it with the notion of job analyzability to define four job classes:<sup>6</sup>

	<i>low job variety</i>	<i>high job variety</i>
<i>low job analyzability</i>	CRAFT (fashion design)	NON-ROUTINE (chief executive officer)
<i>high job analyzability</i>	ROUTINE (assembly line work)	ENGINEERING (mechanical design)

The contention between the interests of employers and the interests of employees is caused by the need for control. Corporations wish to control their business processes, and individuals wish to control their privacy.

The key idea here is that electronic monitoring is an *analysis tool* that is used to adjust the *control mechanisms* that are used to *reduce variety* in business processes. Rather, electronic monitoring is used to mitigate the uncertainty that the human element adds to the business process. The immediate result is that a different level of electronic monitoring is appropriate for each different job class.

---

<sup>6</sup> Hari Das; Strategic Organizational Design; Prentice Hall Incorporated, 1998; page 131.

The CEO of a company does tasks with low analyzability. (It would be difficult to replace a CEO with a computer-controlled robot.) Thus, using electronic monitoring is a poor way to determine when to set controls on his behavior. If electronic monitoring is applied to the CEO, then an inaccurate analysis may result in controls that unnecessarily decrease his freedom. This will inhibit his ability to do high variety work. It is therefore inappropriate to electronically monitor non-routine jobs.

A call-center receptionist does a highly analyzable job. Thus, electronic monitoring is an appropriate method by which to set controls on his behavior. Given that the job has low variety, controls are likely to correct substandard job performance. It is therefore appropriate to electronically monitor routine jobs.

It follows that limited electronic monitoring is appropriate for craft and engineering jobs. In the former case, it is because the *analysis tool/control mechanism* relationship is weak. In the latter case, it is because *control mechanisms* are unlikely to positively affect the quality of work.

There is a natural intuition to this argument. If you were to call a CEO and a telephone receptionist, then whose line is more likely to be “monitored for the purposes of quality control”, and who has the greater claim to privacy?

## 5.0 Conclusion

Electronic monitoring is becoming a standard business practice because it is a cheap and relatively effective method by which employers can control employees. Electronic monitoring does, however, violate the privacy of employees to various degrees.

This paper suggests that business interests and personal interests can be balanced if the type of job being monitored determines the degree to which it is monitored.