Some Problems with Employee Monitoring

Kirsten Martin
R. Edward Freeman

ABSTRACT. Employee monitoring has raised concerns from all areas of society – business organizations, employee interest groups, privacy advocates, civil libertarians, lawyers, professional ethicists, and every combination possible. Each advocate has its own rationale for or against employee monitoring whether it be economic, legal, or ethical. However, no matter what the form of reasoning, seven key arguments emerge from the pool of analysis. These arguments have been used equally from all sides of the debate. The purpose of this paper is to examine the seven key arguments that have been made with respect to employee monitoring. None of these arguments is conclusive and each calls for managerial and moral consideration. We conclude that a more comprehensive inquiry with ethical concern at the center is necessary to make further progress on understanding the complexity of employee monitoring. The final section of this paper sketches out how such an inquiry would proceed.

KEY WORDS: business, employee monitoring, ethics, monitoring, privacy, technology

Introduction

The purpose of this paper is to examine seven key arguments that have been made with respect to employee monitoring. None of these arguments is conclusive and each raises important managerial and moral consideration. We conclude that a more comprehensive inquiry with ethical concern at the center is necessary to make further progress on understanding the complexity of employee monitoring. The final section of this paper sketches out how such an inquiry would proceed.

Arguments

Employee monitoring has raised concerns from all areas of society – business organizations, employee interest groups, privacy advocates, civil libertarians, lawyers, professional ethicists, and every combination possible. Each advocate has its own rationale for or against employee monitoring whether it be economic, legal, or ethical. However, no matter what the form of reasoning, seven key arguments emerge from the pool of analysis. These arguments have been used equally from all sides of the debate. None of these arguments is conclusive and each raises important managerial and moral issues.

The productivity argument

The productivity argument answers the question, "Does employee monitoring lead to higher productivity?" The reasoning begins by viewing monitoring both as a productivity and cost containment tool. First, organizations argue for monitoring as a productivity tool. Many organizations decide to monitor employees in an attempt to keep the employees' personal computer use to a minimum. Surfing the Internet and sending personal e-mails takes up time and reduces productivity. In 2001, 60.7% of employees surveyed said they visit Web sites or surf for personal use at work (WebSense, 2001). Every minute spent booking a flight or checking a stock price is a minute not spent increasing revenue. The computer has usurped gossiping in the coffee room or talking on the telephone as the leading waste of corporate time.

However, opponents to employee monitoring

Journal of Business Ethics **43**: 353–361, 2003.

make the opposite argument. Surveillance can have a negative impact on productivity. Studies have demonstrated a link between monitoring and psychological and physical health problems, increased boredom, high tension, extreme anxiety, depression, anger, sever fatigue, and musculoskeletal problems (Hartman, 1998). Invasive surveillance and monitoring has also been found to lead to higher levels of stress and greater incidence of other physical disorders such as carpal tunnel syndrome (Privacy Rights, 2001). Further, people under stress are sick more often and heal more slowly, which leads to an increase in sick leave and a decrease in productivity while at work. Opponents argue that invasion of privacy can literally make employees sick and may have a counter effect on the productivity that organizations seek.

Moreover, some view monitoring as a cost containment tool. The cost of telecommunications is forcing employers to reexamine their Internet use. With personal web surfing and large e-mails taking up precious bandwidth, many employers are using monitoring as a cost containment tool. The fewer employees downloading large files and surfing heavy bandwidth sites (e.g. pornography), the smaller the fiber optic pipe needed to handle the traffic and therefore the lower the telecommunication expense. Certain software products are designed for this purpose. For example, SmartFilter from Secure Computing disrupts the actions of the user by slowing the download of large MP3 files. The goal of the program is to frustrate the user thereby making such downloads less likely in the future.

The security argument

The security argument answers the question, "Does employee monitoring lead to greater organizational security?" With a greater reliance on computer systems, information assets are seen as a vulnerable point of attack by would-be saboteurs. Corporations that do not adequately secure their systems risk unwanted dissemination, retrieval, or modification of private corporate information. One hacker or virus can bring operations to a halt or cause a large public relations snafu. In such a scenario, proponents argue that monitoring employees protects the safety and security of the organization and even the nation.

Employers feel increasingly susceptible to security concerns. Disloyal employees are able to e-mail trade secrets and confidential documents quickly and easily to a large audience. In fact, most security breaches come from knowledgeable insiders – not random hackers from the outside (Schulman, 2001). By monitoring Internet usage and content, corporations argue that they are able to detect and halt security breaches. Plus, the mere knowledge of increased surveillance may deter potential employee theft.

In addition, many corporations are citing national security issues when determining electronic monitoring methods. Such corporations (telecommunications, chemical plants, oil & gas, banks, etc) see themselves as potential targets of terrorist attacks due to their proliferation and importance in the lives of U.S. citizens. This is not new – many telecommunication switch sites look more like military bunkers than business assets. However, corporations' reliance upon information technology for the maintenance of their assets leaves them particularly vulnerable to attack by electronic means. Electronic monitoring is another "bunker" to maintain the security of their organization.

The liability argument

The liability argument answers the question, "Does employee monitoring lessen employer liability for employee actions?" More than two-thirds of respondents in an AMA survey claim that concern over lawsuits is very important in the decision to monitor (Swanson, 2001). Employers find electronic monitoring particularly helpful in combating sexual harassment and hostile work environment lawsuits; harassing e-mails and surfed porn sites are often probative in harassment cases. In fact, as seventy percent of porn traffic occurs during regular business hours – as calculated by SexTracker, a service that monitors pornography site usage (Conry-Murray, 2001) – it is understandable for proponents to

argue for monitoring Internet communication. Further, employers can no longer wait for the initial complaint; recent court decisions have found employers responsible for dealing with sexual harassment even without a complaint. As the burden of rooting out sexual harassment becomes the responsibility of employers, many make a case for continual surveillance in order to curtail inappropriate behavior before it becomes the basis of a lawsuit.

It is not only sexual harassment; employers have become more concerned about illegal uploading or downloading of commercial software and other copyrighted material onto corporate equipment during business hours. In addition, courts are using e-mail messages as evidence. In the *U.S. v. Microsoft* trial, e-mails that employees thought had been erased were introduced into evidence against Microsoft. These erased or deleted e-mails were easily found on backup tapes. In fact, one in ten companies has received a subpoena for employee e-mails and more than eight percent have defended themselves against e-mail or Internet based sexual harassment claims (Piazza, 2002). As a result, many companies have begun using monitoring as a risk management tool in addition to purging back up systems of old e-mails and files (Gilman, 1999).

It is important to note that increased surveillance of Internet and e-mail usage will only make prosecution of transgressions more difficult – it will not stop the wrong behavior. Hence the "liability argument" should not be confused with a nonexistent "*employee* security" argument. Harassment existed before computers and will persist once all computers are monitored. Further, blaming the embarrassing evidence shown at trial on unmonitored e-mail is a bit like blaming Nixon's transgressions on the tape recorder. The media, not the medium, is to blame.

The privacy argument

The privacy argument seeks to answer the question, "Does employee monitoring respect employee privacy?" To answer this question, an understanding of privacy is needed. Privacy is not a novel issue for employee monitoring in particular or for society in general. Exhaustive debates as to the nature of privacy have raged on for years. Some argue for the "control theory" which measures privacy by the amount of control we have over our own information. Others argue for the "restricted access theory" where privacy is characterized by the level of access others have to our information. For example, if a woman were locked in a room, the restricted access theory would have her in a private situation if an outsider had the key to unlock the door. The woman would have not absolute control over the door opening and closing but would still have restricted access and therefore would be in a private situation. The control theory would find this intrusion to be a breach of privacy and would dictate that the woman have the *only* key to unlock the door in order to ensure a private situation. In such a scenario, she would retain control of her access. The control theory allows for the woman to open the door, expose her habits, and still retain her privacy.

In either case, with the advent of data collection and manipulation, information technology has forced people to rethink their concept of privacy. With complete restriction of access both unlikely and unwanted (how else would we order books online with just one click?), the control theory of privacy allows society to determine who has access to what information without unduly undermining privacy. The user, in this case, would use the restriction of access as a tool to control privacy. The control theory of privacy is also illuminating to the issues inherent in employee monitoring.

Opponents argue that employee monitoring decreases the amount of control employees have over their own information through unrestricted access. Even when organizations do not monitor, but set up the system to facilitate monitoring at any time, a breach of control, and therefore of privacy, has occurred. Control theorists contend that employees realize a loss of privacy even when organizations simply have the capability and opportunity to monitor regardless of whether the organization actually uses that monitoring capability. The employer would have the only

key to the woman in the locked room. It is the threat of monitoring that forces a lack of privacy due to a loss of control.

The creativity argument

The creativity argument seeks to answer the question "Does employee monitoring lead to greater creativity?" It is hard to imagine living in a world in which your every word is recorded for analysis. To spend ten hours a day knowing that your keystrokes can be monitored for productivity and your documents analyzed for a psychological profile seems overwhelming. Opponents of monitoring maintain one could not help but think about the potential implications of every action to your permanent record. You might well feel as if your employer was looking for a transgression and waiting to pounce. In such an environment, employers would severely curtail creative thinking, as employees would begin to act and then think in response to the unseen observer.

New, radical, unconventional ideas may be filtered out of communications if the employee is constantly worried what the observer may think. But corporations rely upon creative, new thinking in order to constantly move forward and improve. In fact, most companies work hard to form innovative and open teams to foster creative employees and improved products and services. Innovation comes only from creativity and, it is argued, is in jeopardy when that creativity is stifled with even the threat of monitoring.

Further, most corporations have political agendas, moral values, and social norms by which they live and breathe. Some ask – prod, demand – their employees to give to certain charitable organizations and to lobby for pertinent legislation. If employers are so upfront as to their desire for employees to conform to their political and moral stances, opponents are quick to reason that employees would begin to take such views into consideration when surfing the Internet or sending e-mails if the threat of monitoring exists. Monitored employees would begin to lose their creativity by conforming to the demonstrated desires of the observer.

The paternalism argument

The paternalism argument seeks to answer the question, "Does employee monitoring lead to paternalistic expectations?" While some may hearken back to visions of "Big Brother", a more appropriate metaphor for employee monitoring may be one of strict parents. The intrusion on a normatively private situation plus a symbolic lack of trust combine to form a paternalistic relationship. Opponents argue that the inherent unequal relationship between employer and employees is exacerbated when trust and privacy are doled out like candy. This relationship can have tangible effects: Swiss economist Bruno Frey found that monitoring negatively affected performance by worsening employee morale. The employees tended to see their employers as having low expectations of them and they then lived down to those expectations (Hartman, 1998). These employees began to act like children with parental expectations.

This paternalism deepens with the unequal distribution of monitoring. As organizations dictate their zones of privacy, groups will be placed in different zones through procedures and rules. With the fragmentation of computer systems, executives may remain immune from monitoring under the same guise of corporate security used to monitor their employees. Executives remain on separate computer servers with different rules of monitoring in order to safeguard corporate strategy and high-level communications. Much as a parent dictates specific rules only for their children, employers may tend toward disparate and unequal policies for electronic monitoring.

The effects of electronic monitoring may be more direct than an overall impression of paternalism. Through the decrease in privacy, monitoring can actually push adults to act more childlike further exacerbating the parent-child relationship. As children become adults and are becoming more autonomous, they are afforded increased privacy in accordance to their level of maturity. While the forward progression to privacy and adulthood is understood, Reiman (1995) argues for the opposite denigration as a possibility. The deprivation of privacy can inhibit

maturity and keep the observed in a childish state due to a loss of privacy and autonomy. As such, employees may begin taking on the role of children as their employer decreases their level of privacy.

The social control argument

The social control argument seeks to answer the question, "Does employee monitoring lead to an increase in social control?" Opponents are concerned that monitoring changes the culture of the broader organization by changing both those employees monitored and those not monitored through the very threat of surveillance. Further, monitoring changes the way individuals act when they are not being watched. And, the argument continues, it is not only the immediate organization but also our society that is impacted through this invasion of privacy.

Privacy has always been regarded as an important if not crucial right. The privacy of employees does more than protect information; privacy is so integral to our identity and autonomy, that it has been argued to be a greater good. Johnson (2001) describes privacy as a social good fundamental to our society. As such, privacy is good for its own sake and not merely as a means to protect an individual or to increase productivity.

It is in this capacity that employee privacy and, therefore, monitoring garners the concern of society in general. Surveillance not only stifles creativity, it can actually change the way one thinks and acts. Opponents maintain that the observed begins to think and act in terms of the observer. Every action, thought, and word is analyzed before being acted upon for potential scrutiny by future or current observers. Further, the observer does not even have to exist. The mere possibility of surveillance can cause people's actions, thoughts, and eventually, minds to change.

Jeremy Bentham capitalized on this idea when he proposed the panopticon – a prison in which a ring of inmate cells surrounds one guard tower high above in the middle (Reiman, 1995). The guard is able to see into every cell; however, due to lighting, the inmates are not able to see the guard tower. The advantage of such an arrangement, according to Bentham, is that inmates will change their behavior at the mere threat of a guard's presence. The guard tower does not need to be occupied at all times.

Now others (Reiman; Johnson) have applied this idea to modern technology in a social control argument. For employee monitoring, not only is the physical layout similar (corporate security watching silently in a centralized, unseen room while employees are being watched from their offices), but the concept is the same. Employers are under no obligation to inform their employees of any monitoring. As such, employees have no idea if the guardhouse is occupied and will change their behavior and thoughts at the mere threat of an observer.

Corporations may find this to be a positive side effect. Organizations are striving for risk and cost management and if employees act in accordance with their social norms, so much the better. However, this type of social control can be, in Johnson's word, insidious. The corporation is exerting an enormous amount of social control that cannot be confined to the scope of business thinking and actions. In this way, corporations are not only invading our physical space, they are invading our "private space" (Reiman) where we introduce, entertain, reflect on, and experiment with new thoughts. By encroaching on our personal intellectual space through social control, employers' surveillance is argued to be a form of oppression where by the mere threat of surveillance leads to a lack of autonomy.

Shoshana Zuboff calls this "anticipatory conformity" (Brown, 2000; Zuboff, 1988) where the norms of authority "become so internalized that the socially desirable response is presented in anticipation of the demand" (Brown, p. 4). Anticipatory conformity is used to minimize the chance of unwanted attention by accepting the fact that one is visible. Employees would be afraid to do the wrong thing and arouse suspicion, and their behavior would conform in anticipation to the projected desires of their authority. Further, it becomes difficult to determine when one is being monitored and, therefore, all behaviors

eventually become anticipatory whether under surveillance or not.

Not surprisingly, most maintain that this social control and lack of autonomy undermines our democratic society. As Johnson (2001) argues:

> Democracy is the idea of citizens having the freedom to exercise their autonomy and in so doing to develop their capacities to do things that have not been thought of and to be critical. All of this makes for a citizenship that is active and pushing the world forward progressively. But if the consequences of trying something new . . . acting unconventionally are too negative, then there is no doubt that few citizens will take the risks. Democracy will diminish.

It is more than the individual employee who is impacted by surveillance. Our society needs autonomous people to challenge the status quo in order to function as a democracy. We rely upon new, unfamiliar ideas to spur the society to improve, and such counter-cultural ideas ferment and grow in autonomous people. Opponents maintain that monitored employees begin to change not only their behaviors but also their thoughts and ideas and therefore, lose their autonomy. They "lose [the] interpersonal core that is [the] source of criticism of convention, of creativity, of rebellion and renewal" (Reiman, p. 42). As such, they argue, our society is damaged.

New inquiry

These seven arguments are used by either side in the employee monitoring debate interchangeably. However, it is difficult to combat a social control argument with a productivity argument (although it is done). The efficient organization appears self-serving and ignorant in comparison to the needs of society. Further, the individual arguments cloud the larger ethical implications of this new technology. As is often the case, we confuse the new *technology* with new moral *issues* requiring a novel approach or argument. While the situation and circumstances surrounding a new technology such as employee monitoring may be different, our society's core ethical issues remain the same. We need a more comprehensive approach to thinking about employee monitoring which incorporates the broad ethical implications to our core moral values.

Philosopher Deborah Johnson sheds light on the impact of new technology on ethics. Johnson (2001) views new technology as introducing novel behavior but not fundamentally new ethical issues. Johnson takes a genus-species approach to the issues introduced by new technology. For her the ethical issues of computer and information technology are a "new species of general, or traditional moral issues" (p. 16). As such, the ethical issues or arguments of employee monitoring involve the traditional moral concepts with a new behavior introduced by technology. While employee monitoring may introduce new ways to breach security, waste time, harass colleagues, and track employees, these have all been issues in the past for organizations and society. Employee monitoring merely adds a new dimension by either broadening the scope or speed of the activity.

Johnson's analysis of new technology and its impact on our preexisting moral values illuminates our first step in taking a more comprehensive approach to analyzing employee monitoring. Rather than tackling each new behavior argument by argument, we must start with four key concepts from ethics: self; relationships with others; community; and property. How does our new technology – employee monitoring – affect each of these key concepts? Where do our existing ideas and values function adequately and where do they break down?

Our core concepts surrounding self, relationships with others, and community include:

> *Freedom* – Individuals have a right to basic liberties that are compatible with everyone's having those liberties. How does employee monitoring affect our basic liberties? If autonomy is considered a basic liberty, how do we monitor employees without infringing on their autonomy? How does notification of the manner and breadth of monitoring impact employee autonomy?
>
> *Privacy* – Respect the privacy of individuals so long as there is not great harm at risk. If privacy encapsulates control of information, how do we monitor

employees while maintaining their sense of control? How does notification impact employees' sense of control and privacy? How can we give employees control of their actions and their information within a monitoring system?

Respect – Treat others as ends in themselves rather than as mere means. Treating others as mere means entails getting their permission to do so. If monitoring is a productivity or cost containment tool, are we using our employees as means to an efficient end? If so, have we asked their permission through full notification?

Responsibility – Individuals are responsible for the effects of their actions on others. What is the responsibility of management to understand the effects of monitoring on its employees? Does taking responsibility for the intended and unintended effects change the way we monitor?

Our core concepts surrounding property include:

Responsibility – People and companies are responsible for the uses of their property. Are organizations misusing their property by monitoring their employees' private communications? If employees are misusing business equipment, how does employee monitoring assist in holding employees accountable for their responsibilities?

Use/ownership – People have the right to determine how to use their property. Are organizations merely exercising their right to protect the use of their property through employee monitoring?

Voluntary agreement – People may make agreements with others about how to use property so long as third parties are not harmed. Are employees entering into a voluntary agreement when using their organization's property? Do the employees fully understand the extent and manner of the monitoring when using the property?

Our analysis of employee monitoring in particular and new technology in general allows us to move from *whether* to adopt to *how* to adopt new technology. Business and privacy organizations may use the individual arguments to argue for or against the adoption of employee monitoring. However, there comes a time in the development of a new technology when we need to realize how if possible to incorporate the new technology within our existing moral framework. By asking questions not about legal liability or productivity but concerning our key concepts of the ethical universe, we are able to examine how employee monitoring and existing societal values can coexist.

A more expansive and comprehensive approach to analyzing employee monitoring must include an analysis of our traditional moral concepts of self, relationship with others, community, and property. Each new technology may impact these core values in novel ways, but the moral issues at stake remain the same. By stepping back and analyzing employee monitoring in light of our traditional moral values we avoid the argument of productivity gains versus social control or employee versus employer interests. Rather we view how our new technology can be incorporated into our existing societal values. We need to ask ourselves, "How will this technology allow us to redescribe ourselves and our communities so that we can contribute to human flourishing and retain our core social values?"

Future research questions

Understanding the values and issues at stake in employee monitoring is step one of a longer process. Employee monitoring provides the launch pad for an exploration into social contracts, identity and moral agency, and the general embedded values of technology.

The exploration of privacy plus the related importance of notification naturally leads to a review of the social contract between employer and employee. Notification allows employees to be informed when entering into either a concrete or hypothetical contract. As such, lack of notification comes close to coercion on the part of the employer, as it is not allowing the employees to make an informed decision. The meaning of contract, consent, and coercion rely upon full notification of the situation to both parties.

However, employee monitoring is just one technology impacting privacy and social contracts. Agre and Mailloux (1997) argue for

specific notification in all cases where technology may infringe upon the privacy of people. Without explicit communication, people do not truly understand the ramifications of the technology they are using or adopting. As such, users do not understand what they are agreeing to. Absent explicit and descriptive notification, users may err on the side of believing that, "they know everything we do" (Agre and Mailloux). A higher level of specification allows users to not only fully understand the privacy issues at stake, but also refrain from gross exaggerations. Such exaggerations generalize the issues at hand and allow users to brush off technology's effect on privacy. If one erroneously believes "they know everything we do," the users will not hesitate to use another technology with privacy implications as there will be no incremental damage. In order for users to adopt technologies with full consent, they must be notified of the technology's true implications. Notification becomes integral to social contracts with today's technology in general and with employee monitoring specifically.

As demonstrated by the effect of privacy on our larger society, privacy and monitoring usurps a person's autonomy and can change how users view themselves. By changing not only how one acts but also how one thinks, employee monitoring and privacy violations in general change our identity. William Brown (2000) tackles the role of identity and the privacy effects of modernity on self-identity in his article "Ontological security, existential anxiety, and workplace privacy." In a related vein, the more one loses one's identity, the less responsibility one takes for his or her actions. If seen as a cog in a larger wheel, users will view themselves as having a proportionate level of responsibility for their actions. A similar situation occurs with large levels of automation that cause the user to relinquish autonomy to the system. In the case of monitoring, if users realize a diminished sense of self-identity, they may transfer their previous accountability and moral agency to the organization that is watching them. As such, identity and moral agency are impacted by privacy violations and monitoring policies.

While we understand the concept of monitoring and the issues at stake, there exist values inherent in the *system* and not just the concept of monitoring. Monitoring, by its very nature, can be seen as value-laden. The very fact that employers will track the communications of their employees places employer knowledge over employee privacy. The choice whether, and subsequently how, to monitor becomes a value-laden decision. Not only do technologies have embedded values, but different systems convey their own values through their features and functionality.

In determining how to monitor, an organization adapts the technology's flexible features to suit their community, norms, and culture. However, these initial flexibilities vanish once the technology is implemented (Winner, 1986) and decisions in the design phase become all the more important. With the move to prepackaged monitoring systems, organizations are not in a position to design their own technology. Instead, businesses choose between an array of systems and corresponding features already designed. Therefore, the decision of which monitoring system, and which features, to adopt is value-laden just as the features are value-laden; and determining which features to adopt requires embracing and/or discarding the values of those features.

Understanding the "value-laden-ness" of monitoring and technology in general will lead one to approach the responsibility of corporations in introducing technology to the public or adopting technology for the organization. Each technology, including employee monitoring, has embedded values and the decision to internally adopt or externally distribute the technologies is a decision to adopt or distribute those values.

References

"2001 AMA Survey Workplace Monitoring & Surveillance": 2001 (American Management Association, New York), http://www.amanet.org/research/pdfs/ems_short2001.pdf.

Agre, Philip E. and Christine A Mailloux: 1997, 'Social Choice About Privacy: Intelligent Vehicle-highway systems in the United States', in Friedman, Batya (ed.), *Human Values and the Design*

of Computer Technology (CSLI Publications and Cambridge University Press, Stanford, CA).
Brown, Willian S.: 2000, 'Ontological Security, Existential Anxiety, and Workplace Privacy', *Journal of Business Ethics* (January).
Conry-Murray, Andrew: 2001, 'Special Report – The Pros and Cons of Employee Surveillance' (2001), *Network Magazine*. February 5, 2001, http://www.networkmagazine.com/article/NMG20010125S0011.
Donaldson, Thomas: 2001, 'Ethics in Cyberspace: Have We Seen this Movie Before?' *Business and Society Review* **106**(4), 273–291.
"Employee Monitoring: Is there privacy in the workplace: 2001, http://www.privacyrights.org/FS/fs7-work.htm (Privacy Rights Clearinghouse, San Diego).
Foucault, M.: 1979, *Discipline and Punish: The Birth of Prisons* (Vintage Books, New York), as quoted in Brown, William S.: 2000, 'Ontological Security, Existential Anxiety, and Workplace Privacy', *Journal of Business Ethics* (January).
Gilman, Andrew: 1999, 'Managing the Trend Toward Increasing Use of Electronic Monitoring Tools', http://www.ema.org/restricted/magazine/mmv5n3/managing.htm.
Hartman, Laura Pincus: 1998, 'The Rights and Wrongs of Workplace Snooping', *Journal of Business Strategy* **19**(3) (May–June), 16(4).
Johnson, Deborah G.: 2000, 'Is the Global Information Infrastructure a Democratic Technology?" in Richard A. Spinello and Herman T. Tavani (ed.) (2001), *Readings in CyberEthics* (Jones and Bartlett Publishers, Inc., MA).
Johnson, Deborah.: 2001, *Computer Ethics* (Prentice-Hall, Inc., New Jersey).
Moor, James H.: 1997, 'Towards a Theory of Privacy for the Information Age', in Richard A. Spinello and Herman T. Tavani (ed.) (2001), *Readings in CyberEthics* (Jones and Bartlett Publishers, Inc., MA).
Piazza, Peter: 2002, 'More Companies Monitoring Computer Use', *Security Management* **46** (January).
Reiman, J. H.: 1995, 'Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future', *Computer and High Technology Law Journal* **11**.
Schulman, Andrew: 2001, 'The Extent of Systematic Monitoring of Employee E-mail and Internet Use', Privacy Foundation. July 9, 2001, http://www.privacyfoundation.com.
Swanson, Sandra: 2001, 'Beware: Employee Monitoring is on the Rise', *Information Week*, August 2001, http://www.informationweek.com/story/IWK20010816S0010.
WebSense: 2001, by NetPartner: http://www.websense.com/products/why/stats.cfm.
Winner, Langdon: 1986, 'Do Artifacts have Politics?' *The Whale and the Reactor* (Chicago).
Zuboff, Shoshana: 1988, *In the Age of the Smart Machine* (Basic Books, Inc., New York).

Kirsten Martin
2113 Tarleton Dr,
Charlottesville, VA 22901,
U.S.A.
E-mail: martink02@darden.virginia.edu

R. Edward Freeman
The Darden School,
University of Virginia,
U.S.A.