

PRIVACY AND TECHNOLOGY: INSIGHTS FROM CATHOLIC SOCIAL TEACHING

Eileen P. Kelly
Ithaca College

Electronic monitoring is an extremely controversial area and one of growing public debate. Clearly monitoring can serve legitimate business purposes. However, it also has the potential to seriously erode the human dignity and privacy of those being monitored. The issue of electronic monitoring is examined by analyzing the extent and nature of monitoring of employees and customers, along with the legal and moral issues raised in monitoring.

Technology has developed at an explosive pace in the Information Age. Historically, bricks-and-mortar companies gathered extensive information about their employees and customers. This information was gathered through such venues as performance appraisals, supervisor ratings, data supplied from customers, as well as data obtained from third-party sources, such as credit bureaus, directories, or commercial mailing lists. In the past, information gathering by companies caused only minor concern. In large part, this lack of concern was attributable to the finite limitations of physical data collection and dissemination. Advances in technology, however, have irrevocably altered the information-gathering process. The growth of sophisticated technology now allows the collection, dissemination, and combination of detailed information on employees and customers at previously unprecedented levels. As commerce becomes more Web oriented, and consumers spend more and more time online, the most intimate details of their lives are becoming digitally accessible. Likewise, sophisticated software is now available to monitor an employee's every computer keystroke, to analyze the content of their e-mail, or to monitor exactly how long the employee spends on the telephone. The rapid spread of technology and electronic commerce has created tremendous opportunities for economic efficiency and customer choice. At the same time though, technology poses unparalleled intrusions into personal privacy. This article first examines the issue of privacy in the age of the Internet. Next, the extent and nature of electronic monitoring of employees and customers is discussed. Then, the legal

issues surrounding electronic monitoring of employees and customers are examined. Finally, the ethical aspects of electronic privacy is discussed from the perspective of Catholic social teachings.

Private, Technology, and the Age of the Internet

“A generation or two ago, the data of daily life, to the extent that it was recorded at all, was ‘entered’ on file cards and bond paper, stored in snap-ring binders and file cabinets, and kept under lock and key. Copying information required the use of carbon paper and considerable human effort. A real-time commercial transaction meant pulling cash from your wallet and collecting the change.”¹ The modern workplace is a vastly different place. Advances in technology, combined with the explosion in electronic commerce, allow companies to gather an unprecedented amount of information on their customers and employees. Much of this information is collected without the consent or knowledge of either the customers or the employees.

The right to “privacy” can encompass a wide variety of concepts. Perhaps the most famous definition was expressed by Justice Louis D. Brandeis when he called the right to privacy the right to be let alone. In *Olmstead v. United States*,² Brandeis foresaw how technological change impacted privacy rights. Brandeis noted in his dissent that when the *Constitution* was written; “force and violence” were the only means by which the government could invade a citizen’s privacy by literally breaking down the front door and entering the premises. By 1928 however, advances in technology (such as wire tapping) allowed for more surreptitious invasions of privacy. Brandeis warned that constitutional provisions against unwarranted search and seizure needed to be extended to meet the changes in surveillance technology. Brandeis’s technological predictions were accurate.

In this digital age, privacy can include the right to control facts and information about ourselves, so-called informational privacy. As individuals spend more and more of their lives online at home and at work, technology poses unprecedented challenges to informational privacy. The right to privacy is a growing concern for Americans. Polls consistently show that privacy concerns are at an all-time high. In a recent *Business Week/Harris* poll, 92% of Web users were concerned about Web sites sharing their personal information with other sites. Indeed, 57% of respondents in the *Business Week/Harris* poll said the government should pass laws on how personal information is collected and used.³ One reflection of this concern are the hundreds of electronic privacy bills currently pending before Congress and state legislatures. The following section examines how technological advances enable employers to extensively monitor the activities of their employees.

Extent and Nature of Electronic Monitoring of Employees

In a recent survey of 1,054 member organizations, the American Management Association found that 67 percent of major U.S. firms record and monitor their employees' phone call, internet connections and computer files.⁴ The percentage is expected to increase in the future. As noted in Table 1, the nature and extent of the activity monitored varies. The primary reasons why employers monitor employees are (1) employee productivity issues and waste of company resources, (2) potential legal liability, particularly sexual harassment suits, (3) safety concerns, and (4) prevention against theft or industrial espionage. Employers interested in monitoring employee productivity and efficiency have extensive means by which to measure work activity at the most detailed level. "Electronic monitoring systems, as they are called, allow employers to measure

Table 1
Percentage of Employers Electronically Monitoring
Employee Activities in the Workplace

Employee Activity Monitored	Percentage
E-Mail	27%
Telephone Conversations	11%
Voice Mail	6%
Computer Files	21%
Video Recording of Performance	16%
Tracking Telephone Numbers & Time Spent on Calls	39%
Video Surveillance	33%

Source: American Management Association. More U.S. Firms Checking E-Mail, Computer Files, and Phone Calls, Says American Management Association Survey. Press Release. (April 2000), <http://www.amanet.org>.

employee efficiency in conducting routine duties. For instance, word processing and data entry tasks can be monitored for speed and errors through electronic systems that count keystrokes. The efficiency of phone operators can be checked by systems that clock the duration or count the number of calls in a given unit of time.⁵ Location tracking technology is becoming rapidly available. Many trucking companies use it to “keep track of their fleets, estimate delivery times, locate stolen vehicles, and ensure drivers don’t violate federal regulations governing how many hours they can be out on the road each day.”⁶

As computer and web usage becomes ever more pervasive in the workplace, employers are increasingly scrutinizing employee use of these assets. Employers contend they provide computer equipment and Web access for business purposes, not personal ones. More and more, employers are restricting or monitoring employees’ Internet and e-mail usage. “A recent survey from SexTracker, a firm that tracks online adult content, showed that 70 percent of all porn traffic in the US occurs between 9 am and 5 pm.”⁷ A wide variety of tracking and blocking software now exists to allow employers to track Internet traffic and block access to Web sites. Some employers also monitor employee and computer Web usage as a means of avoiding potentially damaging lawsuits. An employer can be held liable for the actions of their employees if the latter use company equipment to send offensive e-mail or pictures. Offensive e-mails and pornographic images can be used as evidence in a sexual harassment claim against a company.⁸

Safety concerns are yet another reason why employers may engage in electronic monitoring. Video surveillance of parking lots, elevators, and so on can help provide not only a safe workplace but also provide the employer a defense against potential negligence suits. Finally, theft and industrial espionage are growing concerns of employers. Intellectual capital is increasingly important as a source of competitive advantage in the Information Age. Advances in technology permit easy downloading or e-mailing of sensitive information such as customer lists, proprietary software, trade secrets, and so forth. Employers need to be able to protect themselves against such espionage. The following section examines how technology enables business to monitor the activities of their customers.

Extent and Nature of Electronic Monitoring of Customers

The growth of e-commerce has been explosive in the economy. In the first official U.S. government estimate, the Commerce Department announced that U.S. retail e-commerce sales were \$5.3 billion for the fourth quarter 1999.⁹ The explosion in electronic commerce has been accompanied by increasingly sophisticated information-gathering techniques. Technology now permits the

retrieval and linking of personal information from a wide array of online and offline databases to create intimate profiles of an individual customer. On the positive side, electronic commerce and online technology create tremendous opportunities for economic efficiency and customer choice. However, at the same time, technology poses unparalleled intrusions into personal informational privacy.

The electronic monitoring techniques employed, as well as the amount and specificity of information gathered, vary from e-merchant to e-merchant. Information can be collected by the web merchant itself, by advertisers like DoubleClick or by a plethora of web-tracking and analysis services such as Media Metrix and CMGI. Essentially, information is collected either voluntarily or involuntarily from consumers. Consumers and web surfers may voluntarily divulge personal information such as a name, addresses, credit card numbers, and phone numbers. when making purchases online, when accessing a web site through its registration process or in exchange for free merchandise or services.

Information may also be collected from web users on an involuntary and uninformed basis. Anonymous profile data can be gathered whenever a consumer visits a web site. Technology exists to analyze web logs enabling a web merchant to know the type of web browser used, operating system, country of origin, the site last visited, whether this is a repeat visit and the Internet Protocol address.¹⁰ Cookies may be deposited onto a visitor's hard drive that numerically identifies them and tracks their activities on a web site. Cookies recognize the visitor when they return to the site. Usually, the visitor remains anonymous. However, the cookie has the capability to personally identify a visitor if he or she registered by name at the site before or otherwise personally identified them. Additionally, if a cookie is placed on the hard drive from a banner ad, the consumer can be tracked across multiple sites.

E-merchants previously made additional buying suggestions to a customer who purchased a particular item based on what other similar buyers had purchased. Now personalization software is so sophisticated, it can analyze an individual's every online activity and then instantaneously reconfigure the web page layout to an individual's likes and preferences.¹¹ Data mining software, such as Veribrand's LifeTime, builds detailed digital blueprints of a customer's activity online enabling e-retailers to target offers to specific customers.¹² Additionally, the line between offline and online databases is blurring. Involuntary online data collection is often complemented with off line data sources. Information can come from physical sources such as warranty cards, coupons, sweepstakes' entries, or digital sources like web transactions. Information is also purchased from third parties, such as credit card companies.

Motivation for Monitoring Customers.

E-merchants believe that relationship marketing is vital to profitability. Relationship marketing focuses on building relationships one-on-one with consumers. Technology now lets merchants take relationship marketing to new levels by identifying personal needs and then delivering that content or product, such as personalized home pages or news (e.g. my netscape, my yahoo, my qvc, etc.). Companies gain a competitive advantage through more customer loyalty, more satisfied customers, better customer service, less inefficiency and overall profitability.

Another motivation for monitoring customers is the need to attract advertisers. Most consumer web sites depend, in part, on advertising for revenue. Advertisers typically target their ads towards a select audience. Technology enables advertisers on the web to go one step further and fashion their ads to the specific interests of an individual consumer. User specific information collected on the web enables advertisers to do so. Advertising revenue enables many sites to be “free” to the consumers and web surfers.¹³ The legal issues surrounding the electronic monitoring of employees will be discussed in the following section.

Legal Issues Surrounding Electronic Monitoring of Employees

Many employees operate under the mistaken impression that they have a fundamental right to privacy in the workplace. Nothing could be further from the truth. While employees are protected from privacy invasions by the government under the Fourth, Fifth, and Fourteenth Amendments, no such constitutional protection exists in the private sector. Businesses are essentially free to monitor their employees in the workplace. The Electronic Communications Privacy Act of 1986¹⁴ expressly gives private sector employers the right to monitor employee phone calls, e-mail messages, voice mail, computer files, and other communications made on company owned equipment in the ordinary course of business under the Act’s “business extension rule.” “This exception would allow the interception of e-mail and other communications by an employer, provided certain qualifications are met. The employer would have to prove that it had established a monitoring policy and had made certain employees knew about it in advance of the interception, and that the interception was business related.”¹⁵ Private sector employees thus have few protections from employer monitoring. If an employer establishes policies regarding employee monitoring, they are legally obligated to abide by them. Additionally, an employee may be able to bring suit under the common law torts for invasion of privacy for an unreasonable or unwarranted invasion of

the right to privacy. Thus, an employee may have a cause for action if the employer's monitoring exceeds the bounds of decency, e.g. placing video cameras in the lavatories or dressing rooms.

In July 2000, a trio of bipartisan lawmakers introduced S.R. 2898 and H.R. 4908, the Notice of Electronic Monitoring Act¹⁶ in the Senate and House respectively. The proposed legislation would prohibit companies from secretly monitoring employees in the workplace. At the time this article was written, the bill was still pending before Congress. The following section examines the legal issues surrounding electronic monitoring of customers.

Legal Issues Surrounding Electronic Monitoring of Customers

Like private sector employees, customers of private companies have little privacy protection under existing laws. Currently in the United States while specific statutes exist to protect certain classes of data, such as video rentals and fair credit reporting, few other legal restrictions exist on the compilation, dissemination and sale of personal information on customers. Private sector companies are essentially free to share or sell customer, personalized data with other companies. Current federal laws covering Internet privacy are quite limited and directed primarily at restricting the online collection of information from children. Congress recently passed the Children's Online Privacy Protection Act. The latter requires commercial web site operators to provide parents notice of their information practices, to obtain verifiable parental consent before collecting personal information from children under the age of 13, and to give parents control over the use and disclosure of that information. In lieu of government regulation, the Clinton Administration has consistently promoted self-regulation as the preferred means of dealing with online privacy concerns. Not all countries treat information privacy with the self-regulatory approach that the U.S. does. In the European Community, information privacy is a legally protected right. The following section examines some of the ethical aspects of electronic monitoring from the perspective of Catholic social teachings.

Electronic Monitoring and Catholic Social Teaching

From the author's perspectives, there is nothing inherently unjust or unethical in gathering information on employees or customers when appropriate procedural justice safeguards are put in place. Data gathering has gone on from the dawn of commerce. Until recently however, data collection was done on a limited and fragmented basis. What has irrevocably altered this information gathering process, however, is the growth of sophisticated

technology which enables the collection, dissemination, and combination of information at previously unprecedented levels. Technology has substantially altered the relationship between employees, customers and the companies they interact with and tipped the balance in favor of the company's commercial interest versus the privacy interests of employees and customers. This change leaves employees and consumers particularly vulnerable and subject to harm. Just as our legal conceptions of the right to privacy lag behind in adapting to rapid technological change, so do our moral and ethical conceptions of privacy in contemporary social conditions. Needless to say, achieving a consensus over the limits of electronic monitoring and privacy in a technologically based society is a difficult one. Somehow a balance must be struck between the commercial interests of the company and the privacy interests of its employees and customers.

The issue of electronic monitoring is a growing concern in society. It raises a number of serious moral, ethical and legal issues which warrant scrutiny. The application of Catholic social teaching to an applied issue as electronic monitoring is challenging and fraught with imprecision. Nonetheless, certain basic principles from the Catholic social tradition can be drawn upon in addressing the moral issues surrounding electronic monitoring. A number of closely interrelated principles are discussed below: (1) natural law and the right to privacy, (2) the right to private property, (3) the inherent dignity of human beings and (4) just contract.

Natural Law and the Right to Privacy

McWhirter and Bible¹⁷ assert that the concept of natural rights follows from the concept of natural law wherein individuals have certain basic rights because they are human. The Catechism states that "The natural law, present in the heart of each man and established by reason, is universal in its precepts and its authority extends to all men. It expresses the dignity of the person and determines the basis for his fundamental rights and duties."¹⁸ For example, in the United States, natural rights are recognized expressly in the Declaration of Independence pronouncement: "We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness." While stipulated both in the Declaration of Independence and the *Constitution*, the concept of liberty nonetheless remains rooted in natural law rather than creation by government. John Locke enunciated the concept of the natural state as one wherein all power and jurisdiction is reciprocal, no one having more than another.

From a moral and ethical perspective, one could argue that abrogation of privacy rights grants extraordinary power to certain individuals, thereby diminishing the rights of others in society. In the case of electronic monitoring, one could argue that allowing companies the absolute right to electronically monitor in pursuit of commercial interests violates the liberty and privacy rights of their employees and customers. A balance needs to be struck between the commercial interests of companies and the privacy rights of individuals. Given the unequal balance of power in the latter relationship, it may be necessary for government regulation to be invoked to restore balance. As Patrick Lee notes, "...some basic, important moral truths are publicly accessible; they do not require extensive learning, expertise, or faith, to be apprehended. Therefore we can and should defend these truths in the public and political arena."¹⁹

Right to Private Property

In the Information Age, information is a critical source of competitive advantage and can serve legitimate business interests. Databases containing transactional data and customer information are a key business asset in the modern company. Similarly, measures of employee productivity achieved through electronic monitoring can be vital to improving overall organizational efficiency and effectiveness. The Church has historically recognized the legitimacy of ownership of private property. This legitimacy rests in the charge in Genesis to humankind to have dominion over the earth. The ownership of private property is essential for personal and family autonomy and is a basic human freedom. The right to operate a business successfully would be included in the construction of the right to property. The right to private property, though, is not an absolute one. "For what will it profit a man, if he gains the whole world and forfeits his life?"²⁰ God is the source of all possessions. Leo XIII noted in *Rerum Novarum* that man's possessions were not their own, but rather common to all.²¹ "Private property, in fact, is under a 'social mortgage', which means that it has an intrinsically social function, based upon and justified precisely by the principle of the universal destination of goods."²² A company therefore does not have the absolute right to pursue profit maximization at the expense of the community, including customers and employees. In *Centesimus Annus*, John Paul II addresses the role of profit in business as a legitimate indication that the company is doing well. Profits alone, however, are not the only indication of a firm's condition.²³

Inherent Dignity of Human Beings

The Catholic Church's teachings have consistently stressed the dignity of the human being and decried attempts to use human beings as a means to an end. Companies are not free to turn customers or employees into objects to be used for the interests of the business entity. While electronic monitoring can serve legitimate business interests, consideration must always be given to the dignity of the human person in the employee or customer. In *Rerum Novarum*, Pope Leo XIII stated that "It is shameful and inhuman, however, to use men as things for gain and to put no more value on them than what they are worth in muscle and energy."²⁴ A balance must be struck between a company's need to monitor and the privacy needs of employees and customers.

Unfettered surveillance of customers and/or employees can create a culture of fear and distrust. Being constantly watched can be dehumanizing for both customers and employees, particularly when done so without the knowledge and/or consent of the customer or employee. In the workplace and online, constant surveillance can easily create a prison atmosphere akin to Big Brother ultimately eroding productivity, morale, a trust in the company. Man (including customers and employees) is made in the image of God and therefore poses a spiritual dignity which precludes using him solely as a means to an end. John Paul II notes, "In all cases of this sort, in every social situation of this type, there is a confusion or even a reversal of the order laid down from the beginning by the words of the Book of Genesis. Man is treated as an instrument of production, whereas he—alone, independent of the work he does—ought to be treated as the effective subject of work and its true maker and creator."²⁵

Notably, overt surveillance can be just as intimidating as covert. Simon Pickvance, a research fellow at De Montfort University, Leicester, notes that people under constant surveillance suffer from stress-related diseases.²⁶ It is easy to summarily dismiss surveillance in the workplace with the caveat that "if you are doing your job, you have nothing to fear." Advocates of this approach, however, have not been subject to modern surveillance methods whereby every movement is scrutinized under the unblinking eye of the employer. Sophisticated location-tracking technology is quickly becoming available for cell phones, personal digital assistants, cars, trucks, and boats such that an individual can be physically located at all times when using such a device. In brief, constant surveillance is at odds with the principles of human dignity and a free society. Constant surveillance does not provide the conditions for the realization of human dignity and is at odds with psychological well-being. When the surveillance is done surreptitiously, the harm done to human beings is likewise a moral issue. There is a moral point wherein the dehumanizing costs to the individual outweigh the commercial benefits accrued by the

employer. In the drive for organizational efficiency and productivity, many jobs and customer transactions are in danger of becoming intrinsically inhumane. Financial gain should not be gained through the intentional violation of human dignity. Electronic monitoring of customers has the potential to undermine the human dignity of consumers two ways. First, it can reduce the consumer to a lucrative, salable commodity. The only relevant concern a merchant has to this “commodity” is how much profit can be extracted both in terms of transactions completed and salable information.²⁷ The individuals and the details of their lives thus serve commercial interests first and foremost. Second, by its very nature, online surveillance technology can dehumanize a person through its constant surveillance. Again, some balance must be found between the legitimate right of the company to pursue the operation of the business and the moral right of employees and consumers to privacy.

Just Contract and Privacy Concerns

Traditionally the elements of a just contract have included the following ethical dimensions: (1) that the parties be knowledgeable about the terms and conditions of the contract, (2) neither party misrepresents the contractual situation, (3) parties are not operating under duress or coercion, and (4) the contract does not bind the parties to an immoral act.²⁸ Contractual rights and duties presupposes the existence of just background institutions. Without the presence of the latter, validity and enforceability of contractual rights becomes questionable. As noted previously, precious little legal protection for privacy exists in the United States for employees or consumers in the private sector at this time.

Voluntary and Informed Consent

The use of electronic information-gathering techniques raises key philosophical and ethical questions about the nature of freedom and voluntariness. A fundamental tension exists between the legitimate business needs of a merchant to gather information on employees and customers and the privacy interests of the latter. Companies believe it is essential to engage in electronic monitoring to improve organizational efficiency and better serve their customers. On the other hand, many employees and consumers now believe they have lost all control over how personal information about them is used and circulated by companies.

One could argue that an implied contract is formed when a consumer visits a web site or an employee at-will accepts a position with a company. In reference to the employee, the employee implicitly accepts the terms and

conditions of the job, including electronic monitoring. In the instance of a consumer, she provides information in exchange for access to a web site provided by a merchant. Companies contend that this exchange is both voluntary and informed. At a bare minimum from a moral perspective, fairness and justice in market transactions require that the actors be both free and knowledgeable. While an individual makes an active choice to visit a web site or accept a position, he or she nonetheless may not be aware that information is being collected on them as the basis of the exchange.

Lack of knowledge arises in several areas. First in reference to consumers, the Federal Trade Commission reported that only 14% of commercial web sites disclosed to users any information about their collection of personal data.²⁹ In these situations, consumers clearly lack the requisite knowledge to enter into a just contract. Similarly, when employers do not disclose to employees that electronic monitoring is occurring, an employee lacks the requisite knowledge to make an informed decision. Second, when less obvious methods of data collection are involved (such as when a cookie is downloaded into a user's computer or location-tracking technology is deployed in a company-issued cell phone) requisite knowledge is not present. Third, the ability of web operators and merchants to conduct detailed consumer surveillance leaves consumers far more vulnerable than in traditional retailing concerns. Even given that a consumer is on "notice" of providing information via a online registration form, the consumer may still be unaware that their movements on the site are being monitored beyond the overt information provided. A similar argument can be drawn for employees being electronically monitored. Fourth, in regards to consumers, knowledge is often not present at all when dealing with vulnerable consumers, such as children or the developmentally disabled. Indeed misrepresentation ensues in dealing with vulnerable consumers who are enticed to divulge information through imaginary characters, electronic pen pals, and so on, as was often the case on children's web sites until recent legislation limited the ability to collect data without parental consent.

Suggested Guidelines for Electronic Monitoring

To reiterate a point made earlier, from the author's perspectives, there is nothing inherently unjust or unethical in gathering information on employees or customers when appropriate procedural justice safeguards are put in place. Clearly, electronic monitoring serves legitimate business interests. However, a just transaction should be founded on voluntariness and knowledge and give due regard to the human dignity of the parties involved. Electronic monitoring policies should be clearly disclosed to both employees and customers. In regards

to consumers, privacy policies should be clearly and prominently posted on web sites so that consumers will be able to make an informed decision about whether to divulge personal information. The policies should clearly indicate what information is being collected and what will be done with it, including the potential sale of that information to third parties. Consumers should be given the option to opt out of providing information. Periodically, web merchants should notify their customers of their policies in collecting, renting, selling, or exchanging personal data lists. While notice of privacy policies on company sites satisfies the requirement of informed consent for adults, special precautions and moral responsibilities are necessary for sites directed at children.

In regards to employees, employers should have an electronic monitoring policy and put employees on notice that they are being monitored at the time of hiring and whenever the policy is materially changed. Employers should inform employees about what is being monitored, how the monitoring occurs, and how the information is used. If negative job repercussions can occur as a result of the monitoring, employees should be cognizant of the employer's expectations and standards before the monitoring takes place.

Summary

Electronic monitoring is an extremely controversial area and one of growing public debate. Clearly monitoring can serve legitimate business purposes. However, it also has the potential to seriously erode the human dignity and privacy of those being monitored. With ever-increasing technological advances, electronic monitoring will only increase and thus give rise to continuing public debate over its use and effect on privacy. In a democratic society, the right to privacy has never been construed as an absolute one. Thus, some reasonable balance must be sought between the legitimate business interests of companies and the privacy and dignity concerns of their customers and employees.

This article examined the issue of electronic monitoring by analyzing the extent and nature of monitoring of employees and customers, the legalities surrounding such monitoring, and the moral issues raised in its use. The perspective of Catholic social teaching was used to shed some light on the moral issues raised and to pose some possible solutions. As Williams and Houck note: "Discovering creative ways to help others develop their humanity in the business world is often a formidable challenge...Yet this may be one challenge of the Gospel. The person, understood as created for union and friendship with God, possesses a dignity that has its full flowering only in community."³⁰ This is the challenge that lies before us as technology poses new threats and opportunities.

Notes

1. Charles Jennings and Lori Fena. *The Hundredth Window: Protecting Your Privacy and Security in the Age of the Internet*. (The Free Press, New York, 2000), 1.
2. *Olmstead v. United States*, 277 U.S. 438 (1928).
3. Business Week/Harris Poll. A Growing Threat. *Business Week* (March 20, 2000), 96.
4. American Management Association. More U.S. Firms Checking E-Mail, Computer Files, and Phone Calls, Says American Management Association Survey. Press Release. (April 2000), <http://www.amanet.org>.
5. Lee Burgunder. *Legal Aspects of Managing Technology*. (Cincinnati: West Legal Studies in Business, 2001), 492.
6. Mike France and Dennis Berman. *Big Brother Calling*. *Business Week* (September 25, 2000), 94.
7. Higher-Earning Workers May be Worst Offenders in Downloading Porn at Office. Knight-Rider Tribune Business News. (September 18, 2000), 2000 WL 26753642.
8. Jeff Howe. Big Boss is Watching. *Yahoo! Internet Life*. (October 2000), 104-107.
9. United States Department of Commerce News. Retail E-Commerce Sales for the Fourth Quarter 1999 Reach \$5.3 billion, Census Bureau Report. Press Release (March 2, 2000), <http://www.census.gov>.
10. Aaron Grossman. Keep Track of Visitors to Your Web Site. *Lawyers Weekly USA* 98 (1998), B5.
11. W. Bulkeley. We're Watching You. *Wall Street Journal*, (November 22, 1999), R32, R46.
12. Carol Pickering. They're Watching You. *Business 2.0*. (February 2000), 135-136.
13. Kevin O'Connor. The High Cost of Net Privacy. *Wall Street Journal*. (March 7, 2000), A26.
14. The Electronic Communications Privacy Act of 1986, 18 U.S.C s. 2510.
15. Gerald Ferrera, Stephen Lichtenstein, Margo Reder, Ray August, and William Schiano. *Cyberlaw*. (Cincinnati: South-Western College Publishing, 2001), 208
16. HR 4908, *The Electronic Monitoring of Employee Communications and Computer Usage Act*. July 2000. House of Representatives.
17. Darien McWhirter and Jon Bible. *Privacy as a Constitutional Right*. (New York: Quorum Books, 1992), 55.
18. *Catechism of the Catholic Church*. (Washington, D.C.: United States Catholic Conference, Inc.-Libreria Editrice Vaticana, 1994), para. 1956

19. Patrick Lee. Public Philosophy: A Response. *Is a Culture of Life Still Possible in the U.S.? Proceedings of the Fellowship of Catholic Scholars Twentieth Annual Convention*. (South Bend: St. Augustine's Press, 1999), 14.
20. Matthew 16:26.
21. Leo XIII, *Rerum Novarum*, (May 15, 1891), para. 111.
22. John Paul II, *Sollicitudo Rei Socialis*, (December 30, 1987), para. 42.
23. John Paul II, *Centesimus Annus*, (May 1, 1991), para. 35.
24. *Rerum Novarum*, para. 31.
25. *Laborem Exercens*, para. 30
26. Lynne Bateson. Big Brother's Working Hard at Watching You. *Daily Mail*, (July 29, 1999), 1999 WL 21591429.
27. Marcia Stepanek. Weblining. *Business Week*. (April 3, 2000), EB29.
28. Manuel Velasquez. *Business Ethics: Concepts and Cases*, 3rd. (Prentice Hall, Englewood Cliffs, 1992), 79.
29. Federal Trade Commission. *Privacy Online—A Report to Congress*. (June 1998), www.ftc.gov.
30. Oliver Williams and John Houck. *Full Value: Cases in Christian Business Ethics*. (San Francisco: Harper and Row, 1978), 26.

