2008

Ethical and Managerial Implications of Internet Monitoring

Andra Gumbus
Sacred Heart University, gumbusa@sacredheart.edu

Frances Grodzinsky
Sacred Heart University, grodzinskyf@sacredheart.edu

Recommended Citation

Gumbus, Andra, Grodzinsky, Frances. "Ethical and Managerial Implications of Internet Monitoring." *Emerging Business Theories for Educators and Practitioners*. Eds. Maureen L. Mackenzie and Stuart L. Rosenberg. Cambridge Scholars Press, 2008.

CHAPTER EIGHTEEN

ETHICAL AND MANAGERIAL IMPLICATIONS OF INTERNET MONITORING

ANDRA GUMBUS, ED.D.,
AND FRANCES S. GRODZINSKY, PH.D.

Abstract

As Internet use pervades our personal and professional lives, organizations have become increasingly concerned about employee use of the Internet for personal reasons while at work. This has prompted the restriction of the Internet or the limitation of the Internet during work hours. Monitoring of employee Internet and email is another result of this trend. Legitimate business functions such as employee performance appraisal and progress toward goals are served by monitoring. However, poorly designed and communicated monitoring practices can be negative and have perverse effects on employee morale and productivity. Monitoring of employees erodes trust and may be considered an invasion of privacy. In this paper ethical issues surrounding Internet monitoring are explored from two perspectives: university and business use. Survey results from the university perspective are compared with computer monitoring in a business setting. Students feel an invasion of privacy when a university setting monitors computer use; however, they consider the practice of monitoring the workplace an acceptable invasion of privacy. Reasons cited for unethical monitoring at a university or business setting include: payment for the computer, personal property and possession by the student, and limitations of personal freedom, rights, trust and privacy. Reasons cited for the ethical use of monitoring include: academic use of the Internet, workplace requirements and payment for work,

discouragement of hate crimes and terrorism, and university or employer property.

Privacy and Productivity

Employers have a legal right to monitor productivity of workers while workers have the right to be told how they are watched. Justification from the company perspective includes keeping employees safe and data secure (particularly after September 11). Firms can spot warnings of possible sexual harassment, corporate espionage, and flag words like bioterrorism and anthrax. However, they can also monitor job search sites that can alert the company to problems in departments or anticipated turnover. Should the firm be privy to this information or does it violate employee privacy?

In a Harris survey conducted for WebSense a majority of employees would give up coffee before Internet access. Half of 500 employees admitted using the Internet for news (81%) email (61%) banking (58%) travel (56%) and shopping (52%) (Soat 2005). Surreptitious monitoring can and does occur when employees are on company time using company resources, with little legal protection available for employees. WebSense, the producer of the most commonly used monitoring software reports an estimated annual cost of 53 million employees cyberloafing to be $138 billion. A program called Investigator developed by WinWhatWhere Corporation has 100 corporate and government clients in Canada and monitors all activity, including deleted or unsent messages and can scan for words such as "boss" and "union." It is installed after hours as an "upgrade" and cannot be detected by employees. President of the National Workrights Institute, Lewis Maltby stated, "Employers' efforts to prevent abuse often lead to serious invasions of privacy. People are not robots. They discuss the weather, sports, their families and many other matters unrelated to their jobs at work that can be highly personal" (Thibodeau 2000, 37). The proliferation of technology at home and in the workplace has escalated the friction between privacy and productivity. "Whether it's sexual harassment, hate mail, or just goofing off, these new technologies can make it easier for workers

to commit misdeeds – and to amplify their effect" (Van Slambrouck 2000, 92).

The employer has an unchallenged right to monitor the workplace virtually, but the issue of monitoring the home for telecommuters poses a different concern of invasion of privacy, as the home is protected under the Fourth Amendment of the U.S. Constitution from unwarranted searches and seizures. The issue becomes more complex when we examine if the zone of privacy for the home extends to the network used for telework. As teleworkers were not surveyed for this study, a detailed analysis of teleworker rights is beyond the scope of this paper. It is our position that an organization has an obligation to inform employees of their privacy policies when it comes to the workplace. Many companies neither educate employees on Internet privacy issues, nor specify and communicate acceptable Internet usage to their staffs. Typically, in a monitoring situation, a sample of red flag words are scanned in email and may include: porn, sex, promise, guarantee, exceed, beat, sure thing, easy money, medication, patient record, boss, client file, meds, SSN, ID# (Tam, White, Wingfield and Maher 2005). If the word is found in an employee's Internet activity an alert is generated and emailed to the manager. Managers can receive summaries or log onto a web site to view real time Internet traffic. The web monitoring software StellarIM costs companies $8000 (Roberts 2005). Maltby of the National Workrights Institute stated, "you should take your passport when you go to work because all your rights as an American citizen disappear the second you walk through the office door" (Thibodeau 2000, 37). He argues that the protections of the right to free speech, privacy, and freedom from arbitrary punishment are absent in the workplace. Ironically, these freedoms are virtually guaranteed for the top-level executives who are usually immune from workplace monitoring practices. Some view Sarbanes-Oxley as the vehicle for monitoring that is needed in the executive suite (Sandberg 2005). Forrester Research claimed that the growth rate of 30% a year for monitoring at the executive level is driven by corporate compliance to Sarbanes-Oxley as well as the need to eliminate inappropriate content.

Increasing incidences of identity theft, hackers, phishing, pharming, bot networks and other cyber tricks have pushed some

companies into securing their own sites. Identity thieves usurp personal information and it is estimated that only 1 in 700 are convicted if caught. The Secret Service has uncovered 4000 suspects, 1.7 million credit cards numbers, access to 18 million email accounts and counterfeit documents (Grow 2005). While organizational security is a concern to some, identity theft is often caused by the neglectful practices of others that do not safeguard personal information. Examples are: leaving unencrypted information on computers, selling it to criminals, stolen laptops, lost data, stolen UPS boxes with company data, hacking, failure to monitor employees and other cons and scams. Unfortunately, companies are not punished for these practices and the resulting identity theft. Although monitoring the Internet has increased, the last workplace privacy law was enacted in 1986 before the proliferation of the Internet. Since then, the enactment of new bills and laws has met with mixed success. A current bill in Congress proposes fines and other penalties for companies' failures to protect personal information and would require corporations to protect customer data (Levy and Stone 2005). The circulation of internal emails with private payroll and benefits information has revealed weaknesses in the California privacy law (Verton 2004). Bills increasing employee rights have not passed Congress in 1994 and 2000.

Are employers snooping unnecessarily or are they protecting themselves against legal liability? Drawing the line and maintaining a balance between detecting misconduct and protecting rights to privacy can be a difficult balancing act. The International Labor Organization (ILO) reported that big brother jeopardizes employees' health and welfare. Increased stress and adverse working conditions such as lack of involvement and control over tasks, reduced task variety and supervisory support, fear of job loss, and reduced social support can result from monitoring. Excessive monitoring can be counterproductive and result in low morale and depression that affect productivity (Hall 2004). Conley (2004) argued that trusting employees and respecting individual rights is a better path than electronic surveillance. It does not invade privacy and deplete morale and productivity. He argued that if employees

aren't motivated in the first place, then adding surveillance will only make matters worse not better.

Ethics of Privacy and Trust

One meaning of privacy (the right to be left alone) takes on a whole new dimension in the age of technology. Technology invades privacy because control is lost over who has access to personal information. Privacy as a vehicle for respect for persons can be classified as a moral value from a deontological as well as a consequentialist perspective. Privacy can also be viewed as a virtue to be protected and defended as a moral right (Stahl 2004). The issue of monitoring raises an important aspect of the employee / employer relationship with regard to privacy and trust. Employees may view their privacy being invaded by the company practice of monitoring and blocking web sites and emails. It may also be perceived as a lack of trust and can be counterproductive by causing anger among employees who are monitored. Does the company respect employee privacy? If the company has to restrict access should it provide Internet access at all? Will tracking employee activities in virtual space compromise the workplace relationship? Monitoring employees without informing them violates privacy and intrudes upon the sense of security and individuality that is a necessary component of a trusting relationship. While employee autonomy seems to be violated by workplace monitoring, it should be noted that the organization has the difficult task of balancing personal privacy with organizational security. In a previous study (see Grodzinsky and Gumbus 2005), it was found that preserving organizational security based on the common good of the company only worked in very small offices where everyone knew each other.

Taylor (2000) stated that we overt and covert invasions of privacy should be distinguished. Employees are aware that they are being monitored in overt invasions and are unaware in covert invasions of privacy. Taylor (2000) further argued that employees would avoid personal web surfing thereby reducing their individual autonomy if they knew that they were being watched. No loss of autonomy occurs when employees are free to surf the web and are unaware that they are monitored. Passive monitoring may be a

common ground between overt and covert invasions where the company records information on Internet use and email transmissions, but managers will access these documents only if a suspicion of abuse exists. One may argue that the prosperity of the business is more important than privacy and that "if the business goes well, both employers and employees benefit, no matter how much the employees' privacy rights are violated" (Petrovic-Lazarevic and Sohal 2004).

Ladson and Fraunholz (2005) surveyed six large organizations with respect to online privacy attitudes and policies, and the level of employee awareness. The importance of policies as instructional manuals and preventative documents was stressed. The organization's administrators felt that policies on online and offline privacy and acceptable Internet use and email are important to the organization. However, implementing training of employees on these policies was not considered important. Chen and Park (2005) found that control in the electronic surveillance workplace strongly influences trust and concern for privacy. If employees have some control over the surveillance and monitoring equipment it may make up for the loss of trust when implementing monitoring technology. Control is vital to privacy and when employees have control over monitoring technology their privacy concerns are lessened. Control is recommended as a low cost and effective way to reduce privacy concerns.

The Internet should be a positive productivity tool not a liability. In a recent study, managers expressed concern about the social costs of disrupting the relationship with employees by breeching trust, fairness and privacy. The cost spent in time and energy monitoring, interpreting and acting on data on multiple subordinates can also be a deterrent to electronic monitoring. Ethical concerns about secretly monitoring employees were also indicated. It was found that the decision to monitor secretly carries greater risk of a negative reaction of mistrust, invasion of privacy and injustice than informing employees of monitoring activity (Alge, Ballinger, and Green 2004). As improper use of the Internet on company time affects productivity, managers are often given the sole responsibility of dealing with the information received from monitoring software. Stahl (2004) argued that individuals do not

have the power, knowledge or intellectual capacity to objectively deal with these ethical questions involving privacy and information assurance. If managers are not equipped to respond to these difficult issues then who is ultimately responsible? We will examine this question in the next section.

Managerial Dilemmas: Ethical Issues

Keeping employees focused on work related tasks and enhancing productivity are managerial responsibilities. A study of the impact of the Internet on productivity can be instructive for managers by making them aware of the negative effects on productivity and problematic employee behavior (see Grodzinsky and Gumbus 2005). Employees need to feel valued for their work and that they are being treated fairly and justly in the exchange process between manager and employee. Strong cultures with explicit norms of behavior and IT ethical codes of practice are conducive to curtailing cyberloafing. Norms such as reciprocity, explicitly stating tolerable behaviors and consequences in a written and well-communicated policy that governs the use of the Internet will aid managers as they interpret policy. Peterson examined the influence of guidelines and universal moral beliefs on the use of computers in the workplace and found that clear computer guidelines had a positive effect on business professionals with a low belief in universal moral rules. He supports the need for ethical guidelines for computer use as a simple and inexpensive way to discourage the unethical use of computers and educate users to inappropriate use of company property (Peterson 2002).

The ethical culture of an organization is a reflection of the ethical values of the managers and may be stated in an ethics credo or code and reinforced through education of employees to that code of ethical conduct. Ethical codes can be a deterrent to unethical behavior. The punishment of unethical behavior sets a powerful example for employees. However, managers have differing views on what constitutes a breach of ethics and differ in the interpretation of a company code making enforcement a difficult moral choice. Another difficulty is posed by the frequency of technological changes causing differing interpretations on ethical behavior in

eBusiness (Petrovic-Lazarevic and Sohal 2004).

Managers face the dilemma of needing to curtail cyberloafing and not offending or limiting employee freedom. Should managers allow lapses in productivity for the sake of employee satisfaction? In order to answer this question, Urbaczewski and Jessup (2002) studied employee satisfaction with electronic monitoring. They distinguished electronic monitoring (EM) for simple feedback purposes versus monitoring for control, which reported compliance with Internet acceptable use policies. Urbaczewski and Jessup (2002) found less satisfaction with EM for control of cyberslouching and greater satisfaction with EM for feedback that was generally positive and constructive in nature. They recommended a hybrid approach that allowed managers to influence employee behavior in an acceptable way that high performers would tolerate, and that low performers would dislike, with desirable results for management. They suggested that positive forms of monitoring could be more instructive and acceptable to employees than negative forms of monitoring. They recommended that managers might employ different EM techniques for different employees, such as using EM for feedback for high performers and EM for controlling for problematic employees.

Research Results: University

A survey was conducted with 173 Sacred Heart University (2004) students on the topic of Internet monitoring. Both undergraduates and graduate students participated from the US campus as well as the Luxembourg campus. Students were from the following courses: 19 graduate level Luxembourg students taking Team Management, 47 undergraduate students taking Organizational Behavior, 46 undergraduate students taking Computer Sciences, and 61 undergraduates taking Business Ethics. Of the 173 respondents 114 are male and 59 female. Students under age 21 totaled 116 and there were 57 aged 21 or over. Both Business Ethics and Computer Science students had course modules on privacy whereas the Organizational Behavior and Team management students did not. Students were asked to respond to whether they felt that monitoring was an invasion of privacy and

unethical at a university setting as well as in the workplace. Qualitative results indicated an overwhelming response to the feeling that the university has no right to monitor internet use because it limits personal freedom, rights, trust and privacy. Comments fell into four different categories when analyzed for why students thought it was unethical for the university to monitor. These categories are: students pay for the computer so they feel a sense of ownership: it's assumed to be personal property or a possession of the student; it limits personal freedom (rights, trust and privacy); and the Internet is needed for academic use. There were three categories identified in these qualitative comments that indicated an acceptance of monitoring as ethical and needed. These are: workplace requirement; monitoring discourages hate crimes and terrorism; and the final category of the Internet and all computer equipment are Sacred Heart University property and the school has the right to know what students are doing.

University students were asked if monitoring Internet usage is an invasion of privacy at the university and an overwhelming 65% responded yes. For those under age 21, 67% felt this is an invasion of privacy, and for those over 21 years of age 34% responded that monitoring is an invasion. Knowing that the university monitors Internet use causes 31% to admit that this knowledge alters their Internet behavior. When asked if they consider monitoring unethical 57% responded yes. Fifty six percent of students under age 21 felt monitoring is unethical, and 33% of those over 21 felt the same.

When asked if they considered restricting the use of their computers was unethical, 72% responded yes. Of the 72% of students responding yes to the question about restricting use of their computers, there were only slight differences among the men and women surveyed. 77% of males and 61% of females felt the restriction was unethical. When the same question was analyzed by type of student, the results were different and noteworthy. Computer science students who responded that restriction was unethical represent 69% of all computer science students surveyed. For Business Ethics students the percentage was 86%, for Organization Behavior students the percentage was 67%, and for the graduate Luxembourg based students only 37%. Students who

responded yes to both questions about an invasion of privacy and restricting use being unethical were 48% of the surveyed population.

Out of 173 responses, 110 written comments indicated students felt that their privacy was invaded by monitoring. Interestingly, invasion of privacy was more evident and important to the students who had taken course material on privacy in their business ethics and computer ethics courses. Approximately half of the ethics students and three-fourths of the computer science students felt it was inappropriate for Sacred Heart University to monitor their email and Internet sites. Invasion of privacy was most important to graduate students as well. Out of 19 surveyed, 15 responded that it was unethical for the university to monitor.

Research Results: Workplace

In sharp contrast, responses to identical questions regarding monitoring at the workplace are markedly different with respect to perceptions of privacy. Only 32% of respondents felt that workplace monitoring invaded their privacy. Twenty four percent of students under 21 felt monitoring invaded privacy and 15% of those over 21 felt the same. This knowledge affects only 52% of employees' behavior on the Internet. Only 34% felt that monitoring is unethical and 37% think that restricting use in the workplace is unethical as compared to 72% in a university setting. Age differences were not significant as a factor in response to this question. Twenty five percent of those under 21 and 27% of those over 21 responded yes to this question. Women and men were similar in their belief that restriction was not unethical (63%). Thirty six percent of male respondents and 39% of female respondents felt that restricting was unethical. Students believed that their employers have the right to monitor (93 out of 141). In their comments, students stated that employees are paid to do a job, and they should be working while at work rather than wasting employer resources.

Some students reflected on the extent of employer prerogative by indicating the following: "How far will I let a company go until I feel uncomfortable with its actions? If the company regulates my

email or if it regulates my phone calls I would be fine with it. However, once it starts checking my financial background, and asks for private documents I would not feel comfortable." Most felt that employers not only have the right, but an obligation to determine if employees are productive. Out of 46 total comments from business ethics students, 34 comments were in this category. Ethics students also understood the liability of the employer to harassment lawsuits or other liability exposure if employees were unchecked. Some felt that the employer has an obligation to create a code of conduct regarding use of infrastructures that belong to the employer, and the obligation to educate and inform the employee of this conduct code.

Finally, the topic of disclosure was also addressed by survey respondents. Students felt that monitoring must be disclosed clearly to the employee, or it is an invasion of privacy by the employer. Five out of six comments on limitation of freedom mentioned the need to be informed so it is not "sneaky" on the part of the employer.

Research Results: Observations And Implications

The main observation is the difference in attitude regarding the right of employers to monitor but not the university. It is interesting to note that the percentage of students who felt that it was unethical to monitor Internet use in both the university setting and the workplace was only 32%. Clearly, students felt that monitoring is more appropriate at work than in an academic setting. Questions resulting from analysis of the results that merit further investigation are why the reason of "academic use of the Internet by students" is cited so infrequently as a rationale for not monitoring students. Students use the Internet frequently to do research; yet this category was mentioned only 22 times out of 173 responses.

Another interesting research finding emerged from the comments indicating that since radio, TV and books are not monitored, the Internet should not be as well. This faulty reasoning is cause for concern that students do not understand the extent of monitoring that actually does occur on these various media. When using an Ipod or cell phone our music is tracked, when using cable, Netflix or a Tivo, our TV habits are monitored, when using

Amazon to buy books, our purchases are tracked, and even the library has records of the books we read. How else could the advertising industry be successful with direct – to – consumer ad campaigns and personalized emails suggesting products for purchase? An interesting side note: the author worked at a company in the 1990s- Executone Information Systems- that produced a product called the locator system. Employees were located and voice announced as to their location and who they were with by wearing a badge that was read by ceiling monitors. This product was also sold for tracking portable equipment needed in hospitals (portable X-ray machines) and to dissuade theft of computers and other valuable supplies. It was considered by some to be an invasion of privacy and by others to be a productivity enhancement.

Conclusion

In summary, sophisticated monitoring and blocking tools will continue to be used by organizations to solve productivity issues due to Internet misuse. Wen and Lin (1998) recommended the following minimal functional requirements for these tools: prevent web surfing that is not related to business needs and drain productivity, issue violation notices to the user who breaks acceptable Internet use policy, monitor sites by time wasted, time of day and frequent users to analyze network performance. Wen and Lin (1998) also recommended the following components of an Internet policy: determine acceptable amounts of time spent on-line, determine what should and should not be accessed, determine guidelines for downloading, determine what should be done if objectionable material is discovered, state acceptable chat room use, determine if there is an acceptable time of day to be on-line for personal use, and set rules for sending and receiving email. These policies should limit exposure and liability to the company caused by employees surfing the Internet.

Introna (2001) advocated policies associated with workplace monitoring. If an employee accepts a contract that he/she will abide by company policies, and a monitoring policy is in place, then that employee should have no expectation of privacy in the workplace. Using Rawls' theory of justice, Introna (2001) advised policy

development that ensures: the employer has a right to monitor and use the data for the overall good of the organization; also, the employee has a right to secure a regime of control that justifies all monitoring and assurances that data collected will be used fairly.

The Internet should be a positive productivity tool, not a liability. Employees and students need to feel valued and fairly treated in the exchange process between themselves and management. Strong cultures with explicit norms of behavior and ICT ethical codes of practice are conducive to curtailing cyberloafing and Internet misuse. Norms such as reciprocity, explicitly stated tolerable behaviors, and consequences, in a well-communicated policy that governs the use of the Internet, can aid managers and university IT administrators in their relations with their employees and students.

Works Cited

Alge, B. J., G. A. Ballinger, and S. Green. 2004. Remote control: Predictors of electronic monitoring intensity and secrecy. *Personnel Psychology* 57(2): 377-411.

Chen, J., and Y. Park. 2005. The role of control and other factors in the electronic surveillance workplace. *Journal of Information Communication & Ethics in Society* 3(2): 79.

Conley, L. 2004. The privacy arms race. *Fast Company* 84: 27.

Grodzinsky, F., and A. Gumbus. 2005. Internet and productivity: Ethical perspectives on workplace behavior. *Journal of Information Communication and Ethics in Society* 3: 249-256.

Grow, B. 2005. Hacker Hunters: An elite force that takes on the dark side of computing. *Business Week* (May 30, 2005): 74.

Hall, L. 2004. Where to draw the line. *Personnel Today* (June): 16.

Introna, L. 2001. Workplace surveillance, privacy and distributive justice. In *Readings in Cyberethics*, ed. by R. A. Spinello and H. T. Tavani. Boston: Jones and Bartlett.

Ladson, A., and B. Fraunholz. 2005. Facilitating online privacy on eCommerce websites: An Australian experience. *Journal of Information Communication & Ethics in Society* 3(2): 59.

Levy, S., and B. Stone. 2005. Grand theft identity. *Newsweek* (July 4, 2005): 38.

Peterson, D. K. 2002. Computer ethics: the influence of guidelines and universal moral beliefs. *Information Technology & People* 15(4): 346-362.

Petrovic-Lazarevic, S. and A. Sohal. 2004. Nature of e-Business ethical dilemmas. *Information Management & Computer Security* 12(2-3): 167.

Roberts, M. 2005. Untangling web of wasted time. *Security Management* 49(5): 26.

Sacred Heart University. 2004. URL: it.sacredheart.edu/webservices/policies/privacy/index.asp [viewed December 18, 2004].

Sandberg, J. 2005. Monitoring of workers is boss's right but why not include top brass? *Wall Street Journal* eastern ed. (May 18, 2005): B-1.

Soat, J. 2005. Spamming the globe, surfing at work. *Information Week* 1039: 76.

Stahl, B. C. 2004. Responsibility for information assurance and privacy: A problem of individual ethics? *Journal of Organizational and End User Computing* 16(3): 59.

Tam, P., E. White, N. Wingfield, and K. Maher. 2005. Snooping email by software is now a workplace norm. *The Wall Street Journal* eastern ed. (Mar 9, 2005): B-1.

Taylor, J. S. 2000. Big business as big brother: Is employee privacy necessary for a human-centered management organization? *Business and Professional Ethics Journal* 19(3): 13.

Thibodeau, P. 2000. Employer snooping measure nears vote. *Computerworld* (Sep 11, 2000): 37.

Urbaczewski, A., and L. M. Jessup. 2002. Does electronic monitoring of employee internet usage work? *Communications of the ACM* 45(1): 80-84.

Van Slambrouck, P. 2000. E-mail ethics: You've got pink slip. *Christian Science Monitor* 08827729: 92.

Verton, D. 2004. Email glitch exposes flaw in privacy law. *Computerworld* 38(28): 1.

Wen, H. J., and B. Lin. 1998. Internet and employee productivity. *Management Decision* 36: 6.

PART VI

ABOUT THE AUTHORS

Lisa Z. Bain, Ph.D.
Lisa Bain is an Assistant Professor of Computer Information Systems in Rhode Island College's School of Management and has a Ph.D. in Information Systems from Nova Southeastern University. Dr. Bain teaches courses in Computer Literacy, Management Information Systems, and Networks and Telecommunications. Her background also includes over 10 years of industry experience, including work as a Systems Engineer for IBM. She currently focuses her research on E-Commerce usability, improved teaching methods, and Open Source Software.

Frances S. Grodzinsky, Ph.D.
Frances Grodzinsky is a Professor of Computer Science and Information Technology at Sacred Heart University in Fairfield, Connecticut. In 1992, 1994 and 2000, Dr. Grodzinsky participated in ethics workshops sponsored by the National Science Foundation. She has given numerous workshops and presentations at SIGCSE, CEPE, ETHICOMP, APPE and ISTAS. Dr. Grodzinsky's areas of research include virtue ethics, digital divide and community, equity of access, cyberstalking, privacy, and property and fair use. Dr. Grodzinsky is co-chair of the Hersher Institute of Ethics at Sacred Heart University, where she has been instrumental in fostering ethics across the curriculum.

Andra Gumbus, Ed.D.
Andra Gumbus earned her Doctorate in Educational Leadership from the College of Business at the University of Bridgeport. She teaches undergraduate courses in the College of Business at Sacred Heart University in organization management, organizational behavior, and business ethics. Her graduate courses include organizational management and business communication and team management. Dr. Gumbus' research in these areas includes

business ethics, organizational behavior, and performance management. She has published over twenty articles and has presented at over twenty conferences. Dr. Gumbus has received the following research awards: SHU College of Business Research Awards in 2005 and 2003, and the Eastern Academy of Management Conference Best Paper Case Association Award 2003.

Kimberly Killmer Hollister, Ph.D.
Kimberly Killmer Hollister is an Associate Professor in the Department of Management & Information Systems at Montclair State University. Prior to joining the faculty at Montclair State, she held a lecturer position at the Wharton School of Business. Her research falls into two main categories: applied operations management and educational program assessment of management information systems and operations management curricula. Dr. Hollister is the current Treasurer and Past President of the Northeast Business & Economics Association, a member of the Decision Sciences Institute, and serves on the review board of the International Journal of Information Systems and Supply Chain Management.

Joseph Kasten, Ph.D.
Joseph Kasten is an Associate Professor of Computer Information Systems at Dowling College in Oakdale, New York. He earned his Ph.D. from Long Island University's College of Information and Computer Science. His current research interests center on the alignment of organizational knowledge with business strategy. Prior to joining academia, Dr. Kasten was a Senior Engineer for the Northrop-Grumman Corporation, where he helped develop aircraft such as the F-14D and Boeing 777, as well as the International Space Station.

Nicole B. Koppel, Ph.D.
Nicole Koppel is an Associate Professor in the Department of Management & Information Systems at Montclair State University. Dr. Koppel's research focus is in the broad area of assessment in technology and quantitative studies. In addition, she has published in the area of operations management. Her research can be found in