1-1-2005

Legal and Ethical Implications of Employee Location Monitoring

Gundars Kaupins
Boise State University

Robert Minch
Boise State University

Legal and Ethical Implications of Employee Location Monitoring

Gundars Kaupins, Ph.D., SPHR
Department of Management
Boise State University
Boise, Idaho 83725
gkaupins@boisestate.edu

Robert Minch, Ph.D.
Department of Networking, Operations, and Information Systems
Boise State University
Boise, Idaho 83725
rminch@boisestate.edu

Abstract

Location technologies allow employers to monitor the location of employees. The technologies range from global positioning systems able to determine outdoor locations worldwide to sensor networks able to determine locations within buildings. Few international laws and no American laws directly address location monitoring. International privacy laws, the Electronic Communications Privacy Act, the USA Patriot Act and other laws involving Internet and e-mail monitoring might provide the pattern for future location monitoring legislation. Ethical considerations such as privacy, accuracy, inconsistency, security, and reputation also may affect future legislation. In writing corporate policies governing location monitoring, the employer's business interests may outweigh an employee's privacy interest. However, privacy invasion may be considered when the employer's monitoring has been physically invasive and has no legitimate business purpose. Future research should investigate management and employee attitudes toward location monitoring and the pattern of location monitoring policies.

1. Introduction

Emerging technologies are making it possible for an organization to monitor the location of its employees in real time virtually everywhere. These technologies range in scale from the global positioning system (GPS), able to determine location outdoors worldwide, to sensor networks, able to determine location inside building rooms. Location-aware technologies and their privacy implications are reviewed in [34]. Before discussing the legal and ethical implications of location awareness in employee monitoring, the most important technical aspects are reviewed briefly below.

First, individuals are generally not directly locatable through location-aware technologies—they are indirectly locatable because they may be in close proximity to or carrying a location-aware device such as a cell phone. The certainty of a user's location is dependent upon the certainty of a mapping from device to user. Only in the still-rare case of a technology such as a radio frequency identification (RFID) tag [56] permanently implanted in a person's body would direct tracking of individuals be possible. We do not consider non-mobile monitors such as wall-mounted infrared sensors.

Second, location-aware devices are becoming pervasive because of dropping cost, government mandates, and marketplace factors. The cost to make a device location-aware ranges from nothing (in devices already inherently locatable) to a few dollars or tens of dollars when GPS or other location technology must be added. To allow better response in emergencies, agencies such as the US Federal Communications Commission are phasing in requirements that cell phones be locatable [16]. Businesses and consumers are beginning to demand location-aware technologies in the marketplace—for example, it is estimated that up to 80% of new vehicles will come equipped with location-aware technology by 2006 [53]. Estimates of the size of the global location-based services market are 18.5 to 20 billion US Dollars by 2005-2006, with 31% in Europe and 22% in the US [35]. The low cost and pervasiveness of the technology not only mean that employers can easily supply it to their employees, but also that the workers may already be locatable through their own personal (i.e., not work-related) devices—including phones, PDAs, laptop computers, automobiles, etc.

Third, there are numerous location-aware technologies that include greatly differing characteristics such as accuracy (e.g., within a few meters for GPS; within a few millimeters for sensor networks), venue (e.g., outdoors versus indoors), location determination methods (e.g., determined internally by a device itself, or

externally by the systems and/or networks it interacts with) and operational modes (e.g., actively and continuously tracking versus passively responding to point location requests only) [34]. Even if a device is not designed to be location-aware, it may be locatable. Wireless local area network (WLAN) technologies using fixed access points with a range of only 50 to 100 meters make all users of the WLAN locatable by virtue of their association with the access point.

Finally and most importantly, location information may be processed and combined with other information to allow a great number of inferences that concern much more than mere location itself. Noting locations at two points in time may allow a trucking company to infer in one case that its driver is napping, and in another case speeding. Comparing location records for two employees can be used to infer whether or not they had the opportunity to directly exchange company property. We will address many more examples of these inferencing issues later.

2. Purpose

In following sections, we will examine a number of important legal and ethical implications of employee location monitoring. While the technologies and issues are global in scope and we will note some international dimensions, we will focus on the United States for many of our examples of existing laws and policies. Legal and ethical issues lead to policy implications for organizations. We will give examples of these implications and make suggestions for policy responses.

3. Existing law

The right of an individual (whether she be an employee or not) to location privacy has not been clearly established anywhere in the world. An attempt to codify such a right by the US Congress, the Location Privacy Protection Act of 2001 [55], was proposed but not passed into law. The Norwegian Personal Data Act [40] requires consent for processing sensitive data said to include location data [48] although the English translation of the act does not contain the word "location." The Finnish Personal Information Law and Law about Privacy and Security of Telecommunications are said to be applicable to location privacy although "there are no laws in Finland that actually concern location information" [27].

Similarly, in the US no laws directly address employee location monitoring [53]. However, in general, employers have considerable freedom in monitoring employees' work as an extension of the right to control business functions such as customer service and assembly line productivity. The freedom is not total because laws and court decisions attempt to strike a balance between the need to gather information about employees to improve profitability or reduce liability and the need to protect privacy and reduce discrimination [39].

One way to analyze how employee location monitoring is appropriate or inappropriate is to investigate parallel employer behaviors associated with employer monitoring of the Internet, E-mail, and regular work behavior. Many of the location monitoring laws in the future may be extensions of existing laws associated with computer, video, and audio monitoring of employees.

3.1 International and US laws potentially encouraging the use of employee location monitoring technologies

International Privacy Laws. A survey by Privacy International and freedominfo.org found that fifty-seven countries, mostly from Europe and North America, have passed privacy and freedom of information legislation. Thirty-seven countries, mostly from Africa and South America, have pending efforts. Though this legislation focuses on making governmental information more available across national and international boundaries, there is a considerable attention to defining personal data privacy. Personal data is defined as any information relating to an identifiable individual [5].

The Organization for Economic Co-operation and Development (OECD) developed influential personal privacy rules under the 1980 OECD Privacy Guidelines, the 1985 Declaration on Transborder Data Flows and the 1998 Ministerial Declaration on the Protection of Privacy on Global Networks. The OECD guidelines encourage the transfer of personal data across countries in order to enhance business and economic relationships [41].

In 1995, the European Union passed Directive 95/46/EC that embodied many of the principles of OEDC guidelines. [13]. Australia and Canada developed similar personal privacy laws that are often used as models for common law countries [5]. The Australian Privacy Act of 1988 and the Canadian Protection of Personal Information and Electronic Documents Act of 2001 provide governments and companies wide discretion on the types of personal data that may be collected [13].

Though OECD guidelines prohibit the secret collection and use of personal data, Canadian privacy law permits such collection and use if it is in the interests of the individual, is reasonable for investigating a breach of agreement or law, the information is publicly available, a life-threatening emergency occurs, or it is used for scholarly research [13].

Electronic Communications Privacy Act (ECPA) of 1986. On the surface, the US ECPA provides limitations on the use of computers to monitor employees. The act prohibits unauthorized access of the contents of stored

wire and electronic communication. The act specifically covers e-mail, Internet chat, and voice mail. No mention of location technologies is made but many of the principles of this act may eventually apply through court decisions and legislative amendments. The act is noted for its four exceptions to its main prohibition [25], virtually assuring employers that electronic communication interception is protected [39]:

1. Consent Exception: Employers should have clear policies on monitoring and employees must consent to the policies.

2. Provider Exception: Employers may provide employees with monitoring equipment to ensure quality service and reduce the chance of theft.

3. Business Use Exception: Monitoring can be done for business-related activities [39].

4. Government Use Exception: The government may order the employer to disclose contents of computer communications with warrants or subpoenas to deal with emergency situations [25].

With these exceptions, it may be possible to extrapolate the law to conclude that if location monitoring devices are used based on clear policy and consent of the employee (consent exception), the employer provides the location monitoring devices (provider exception) for business purposes (business use exception), there may be potential support for the use of the devices. Furthermore, information obtained from location monitoring devices could be provided to the federal government (government use exception).

Civil Rights Laws. Based on the Civil Rights Act of 1964 and interpretations from the Equal Employment Opportunity Commission (EEOC), sexual harassment involves "actions that are sexually directed, are unwanted, and subject the worker to adverse employment conditions or create a hostile work environment" [31, p. 178]. According to the EEOC, employers are legally liable for sexual harassment issues in the workplace if they should have known about sexual harassment and they did nothing about it.

An employee, for example, could be accused of sexually harassing other employees at a particular business location not associated with his or her normal work location. If an incident occurs and monitoring technology places the employee in the unauthorized location, this may be further evidence of sexual harassment.

Unauthorized entry into employee records rooms or files could be associated with illegitimate release of health records, polygraph records, and demographic characteristics such as age. It could be discovered, for example, that an employee has had AIDS or cancer. Mistreatment of that legally-protected employee could be a violation of the Americans with Disabilities Act (private sector), Vocational Rehabilitation Act (public sector) and the Health Insurance Portability and Accountability Act. Mistreatment by race, religion, gender, color, and national origin could be a violation of the Civil Rights Act of 1964. Mistreatment by age could be a violation of the Age Discrimination in Employment Act of 1967. Mistreatment by pregnancy might be a violation of the Pregnancy Discrimination Act.

National Labor Relations Act (NLRA). Interpretations of the NLRB from the National Labor Relations Board (NLRB) state that employees may be prevented from distributing literature in working areas at any time. They may not be prevented, however, from making distributions in nonworking areas on nonworking time. The solicitation restrictions may be in force as long as it is applied without discrimination—meaning that unions should not be singled out as the only group with restricted solicitation [11]. Location monitoring could provide some evidence that employees went throughout the company to distribute union materials at an improper time. Any grievance committee, however, would have to distinguish between coincidence and cause concerning material distribution

Occupational Safety and Health Act (OSHA) of 1970. OSHA encourages employers to monitor safety practices in the workplace. Monitoring of employee location could help companies enforce the Act. For example, a paint room door could be opened and an employee could inhale toxic fumes. He or she could try to quietly leave the room without the company knowing about it. With a location monitoring system, the company could know who the employee was and address the safety concern.

USA Patriot Act. This act makes it easier for the federal government to gain access to company-held records of employees, which could include location information. The government does not have to show evidence that employees are "agents of a foreign power," that there is reasonable suspicion of criminal activity, or that there is probable cause for suspicion under the Fourth Amendment to the Constitution. The government must merely show that any information requests are related to terrorism or foreign [3].

There is potential that the Federal government might request business-related and personal data associated with employee location at any time. There also is potential that the government might request that companies monitor employee locations for investigative purposes.

Economic Espionage Act of 1996. This act enables the federal government to prosecute individuals who convert trade secrets for their own or others' benefit with the knowledge or intention to cause injury to the trade secret owner [12]. Confidential business information is treated as a property right [49], and location-based evidence of a company employee meeting with a

competitor without authorization might be used as evidence of a violation.

Criminal Laws. Location monitoring is already being used to prosecute employees for criminal acts. Four New Jersey police officers recently pleaded guilty to filing false records after GPS tracking devices were installed on their patrol cars in 2001 and used to provide evidence that the officers were not conducting patrols as they reported [18]. Employee location monitoring records could be subject to subpoena in criminal cases, and could also be used to prove innocence instead of guilt. If a victim accused an employee of assault, for example, the time-stamped location records of the employee could provide exonerating evidence if both parties were never in the same location at the same time.

3.2 International and US laws potentially limiting employee location monitoring

International Laws. The 1980 OECD Guidelines, inspiration for European Union, Canadian, Australian and other international laws, include specific allowances for personal data collection. These could be applied to location monitoring.

1. Collection Limitation Principle: Data should be collected by lawful and fair means with the knowledge of the individual.
2. Data Quality Principle: Relevant data should be accurate, complete, and up-to-date.
3. Purpose Specification Principle: The purposes of data collection should be specified.
4. Use Limitation Principle: Data should be disseminated only based on an individual's consent and legal purposes
5. Security Safeguards Principle: Data should be protected from loss, misuse, or modification.
6. Openness Principle: There should be general openness in the collection and use of the data.
7. Individual Participation Principle: Individuals should have a right to know how personal data is collected and by what means.
8. Accountability Principle: Data collectors should be accountable for their data sets [41].

Electronic Communications Privacy Act (ECPA) of 1986. The ECPA potentially could place limits on location monitoring through its discussion of exceptions. If a company does not inform employees (consent exception), use its own equipment (provider exception) and use monitoring for business purposes (business purpose exception), then there may be a case against location monitoring.

Court decisions have ruled that the employer's business interests outweigh an employee's privacy interest. Furthermore, courts have upheld claims of invasion of privacy only where the employer's monitoring has been physically invasive and has no legitimate business purpose [38].

Civil Rights Laws. Employers might know that some employees have cancer, are getting divorces, and are HIV-positive [20]. Some of this information can potentially be inferred by knowing the location of the employee. For example, an employee might be going to a breast cancer ward in the hospital every week. Such trips may or may not be an indication that the employee has breast cancer. The person could be visiting a friend, doing volunteer work, or eating in a cafeteria that is near the ward. This could be a violation of the Americans with Disabilities Act.

A "secretly" pregnant woman could be discovered going to a pregnancy clinic. The employer might conclude that the woman is pregnant based on trips to that clinic and accordingly affect employment decisions based on that secret information. This could be a violation of the Pregnancy Discrimination Act.

National Labor Relations Act (NLRA). The NLRA and interpretations from the National Labor Relations Board (NLRB) set limits on company monitoring of union activities of union and potential union members. According to the NLRB [46], an employer who accidentally and casually observes a union meeting might not be a violation of the NLRA. However, if the employer observes who is at the meeting, asks specific questions to subordinates about the conclusions of the meeting, and follows the meeting with mandatory questions about the meeting, there probably would be a violation of law [17]. Location monitoring could potentially be a violation of the NLRA because employers could know exactly who attended union functions and what time.

Location monitoring has already been the subject of labor contract negotiations. United Parcel Service (UPS) Teamsters union member workers successfully included a contract provision in 2003 prohibiting the company from using GPS data in employee evaluations, and snowplow drivers in Massachusetts have protested a requirement that they carry GPS-equipped cell phones on their routes [53].

4. Ethical issues

Another way to analyze how employee location monitoring is appropriate or inappropriate is to investigate the ethics of employer behaviors associated with employer monitoring of the Internet, e-mail, and regular work behavior. Ethics is a discipline that either supplies or justifies a coherent moral system of thinking and judging (normative perspective) or describes the morality of a culture or society (descriptive perspective) [51]. This paper focuses on the descriptive perspective by addressing research on ethical considerations such as

security, productivity, reputation, impact on third parties, privacy, accuracy, inconsistency, right to examine records, and informed consent.

4.1 Ethical considerations encouraging employee location monitoring

Security. Companies often experience questionable employee activity. For example, according to one survey, the number of employees sharing confidential business information via e-mail with other companies is about 26 percent. The same poll found that nearly three quarters of respondents sent or received adult-oriented e-mail at work [7]. Just as company email is commonly monitored, location of employees might be monitored to discourage and detect possible unauthorized disclosure of confidential information to competitors.

Another security concern is that employees might be in parts of the company where they are clearly unauthorized. Parallel company restrictions include having keys to doors and files and providing cascading passwords to go into various computer files [1]. Some of the unauthorized locations could be the company's bank vault, employee records rooms, and bathrooms (e.g., men in women's bathrooms).

Productivity. Businesses historically have had a right to improve employee performance. An aspect of employee performance is being at the right place at the right time. For package delivery firms, monitoring the locations of trucks and delivery personnel can help dynamically adjust routes and otherwise improve customer service.

Businesses also historically have had the right monitor employee efficiency. They are concerned with determining the length of time employees work on certain projects to assess project costs and reduce wasted time [32]. Organizations are concerned about Internet and e-mail mostly to protect their investments, assure a safe and hospitable working environment, and provide quality services to customers [14] [4].

Location monitoring technologies may be seen as just another means of improving employee performance and efficiency. Vendors of systems that allow such monitoring are using this as a selling point [23], promising reduced overtime, down time, time spent in unauthorized locations, and employee fraud.

Reputation. According to the e-policy institute, employers wish to maintain their professional reputation [43]. Employers may not want employees with company logo to go to casinos, bars, or other places where the employer may be embarrassed.

Impact on Third Parties. Intrusions into an employee's privacy for the sake of protecting third parties are justified by four criteria:

1. The third party's interests (e.g., health and safety) are protected when the employer is morally responsible.
2. The means chosen are efficient to obtain the required information.
3. The least intrusive means to obtain information are chosen.
4. The intrusion on the employee is not so severe as to outweigh the third party interests [42].

Persons not covered under the employer's contract such as customers, shareholders, suppliers, creditors, workplace neighbors, relatives of workers, and others may be impacted by the actions of employees. Employers can be liable for the actions of employees on others [42]. For example, an employee with a history of sexual harassment against a customer could be subject to a restraining order prohibiting the employee from approaching that customer, with location monitoring systems verifying compliance.

4.2 Ethical considerations limiting employee location monitoring

Privacy. Privacy rights exist under the Fourth Amendment in the US and under various laws worldwide, particularly when a person has a subjective expectation of privacy and society accepts that as reasonable. Employee privacy rights and reasonable employer rights may need to be balanced on a case by case basis [28] [36] [33].

During the course of a day, an employee may go to business-related places and non-business-related places. A trip to a bank to deposit coins might be of legitimate interest for those monitoring employee location. However, monitoring a personal trip during a lunch break might be an unreasonable intrusion on employee privacy. According to Candice Johnson, assistant director for the Communication Workers of America, top management might not be able to resist using location monitoring to create oppressive work environments. Companies that limit restroom time to 15 minutes might now be able to check how long employees were in the restroom [23].

Accuracy. Location-aware devices will never provide perfect information about employee location. Most systems such as GPS have inherent accuracy limitations, may suffer from signal loss interrupting operation, may be subject to incorrect configuration by operators, and may of course simply malfunction. Inaccuracies of even a few feet could make the difference between an employee being accused of wrongdoing or exonerated.

Monitoring of employee location is dependent upon a location-aware device being associated with that employee. This may be intentionally subverted by a dishonest employee. For example, to hide a trip to an unauthorized location, an employee could secretly give

the location-aware device to another employee who would complete an authorized route. Even unintentional misplacement of location-aware devices could cause concern. Devices not carefully safeguarded could be stolen and used for fraudulent purposes.

Even if location-aware device is properly associated with and establishes an employee to be at a certain location at a certain time, care must be taken to avoid assumptions of improper behavior based on circumstantial evidence alone. An employee may have traveled to a competitor because he or she was merely talking to a friend. An employee may have stopped his or her car near a bar because there was a malfunction in the car and not because he or she was visiting the bar. Employers might be held liable for firing employees based on false rumors employers illicitly received.

Inconsistency. In any employee grievance case, the hot stove rule is a major defense for the company. In the hot stove rule, discipline should be immediate, consistent, impartial, and with a warning [10]. A major concern of computer monitoring in general is the consistency in discipline. Companies will often provide immediate discipline for employees who engage in one prohibited activity (e.g., accessing pornographic Web sites) while not enforcing the same discipline for other prohibited activities (e.g., illegal gambling and playing games) [39]. Whether these violations are equivalent is subject to interpretation. Location monitoring may play a part in the inconsistency issue, since any prohibited locations for employees could at least be uniformly defined and infractions consistently detected.

Right to examine records This right is part of the guidelines from the OECD and included in the fifty-seven international laws passed involving freedom of information [5]. The data concerning location monitoring might need to be revealed to employees to confirm that they have completed their trucking or other business routes. Some other employee purposes of examining location records may include confirming the location of employees during alleged crimes, revealing management misbehavior in terms of using location information, and understanding the best routes and schedules.

Informed consent This right is also part of the guidelines from the OECD and is included, with occasional constraints, by fifty-seven international laws on privacy rights [5]. A major concern with employee location monitoring is secret monitoring especially in potentially private and non-job-related places such as bathrooms and clinics.

5.0 What employers should do: policy manuals and employee handbooks

Specific Examples of Policies. Five sets of researchers and organizations have contributed to policies associated with electronic employee monitoring. None have directly addressed location monitoring but the principles could likely be applied in this new area. They include employee handbook experts [2] [9] [7] [15] ethics code developers [19] legal researchers [13] [42] [54] [29] [11] [8] [37] [47] [45], international organizations [41] [38] and international and state governments [13] [50].

Dimensions of Location Monitoring Policies. The researchers and organizations mentioned above have provided a variety of ways to look at location monitoring based on their recommendations for computer monitoring in general. Legal monitoring policies tend to be associated with several dimensions—how monitoring is set up, how monitoring is communicated, how discipline is applied, and how the impact of monitoring is analyzed. Each dimension can range from no activity to intense action. Table 1 shows solutions to basic questions associated with the four dimensions based on the literature.

Table 1—Suggestions for Location Monitoring Policies

Dimension	Questions	Sample Solutions
Set up	Who will do the monitoring?	Supervisors, top management, IT director [9]
Set up	What equipment will be used?	GPS and RFID technologies [23]
Set up	What/Who will be monitored?	Information is collected on an equal basis across all employees. Ban the collection of data unrelated to work performance [3] [39]
Set up	When will monitoring take place?	On company time [2]
Set up	Where will monitoring be allowed?	Monitoring should be limited to the workplace [20] [38] Monitor what is relevant [23].
Set up	What specific behavior is allowed?	Communications and information exchanges directly relating to the mission, charter and work tasks of the organization. [50]

Set up	What specific behavior is not allowed?	Giving information to competitors [44] [39]
Monitoring Set up	How are policies coordinated?	Integrate e-mail, location monitoring, and other technologies into one policy [3] [39]
Communic ation	Who will be warned of monitoring?	Use covert monitoring only when there is evidence that a crime has been committed [19] Avoid any covert monitoring [24] [38]
Commun-ication	By what means will monitoring be announced?	Employee handbooks, letters of understanding, e-mails [7]
Commun-ication	When will monitoring be announced?	A reasonable time before monitoring begins [41]
Commun-ication	What reasons will be given for monitoring?	Major reasons may include productivity and security [23] Sexual harassment [11]
Discipline	Who will discipline workers for going to incorrect locations?	Supervisor [9] [4] [21]
Discipline	What are the different types of disciplines associated with location?	Apply progressive discipline [9]
Discipline	What can employees to do appeal their discipline?	Give employees the right to dispute electronic monitoring data [3]
Discipline	What about retaliation from any party?	Provide a non-retaliation policy [3]
Impact of Location Monitoring Procedures	Who will monitor the results?	Top management or data collection experts [41]
Impact of Location Monitoring Procedures	By what means will location monitoring be analyzed?	Analyze the impact of monitoring (19] Develop a comprehensive records retention policy [39]

Set Up. The first major dimension refers to what is monitored or restricted. Kevin Conlon, district counsel for the Communication Workers of America asserts that monitoring should be limited to the workplace. Only information relevant to the job should be collected. Monitoring should result in the attainment of some business interest [20].

Communication. The second dimension refers to communication of the policies with employees. Though monitoring is on the rise through available technology and with some legal support, many employees are kept in the dark about how and when they are monitored. Four out of every ten employees do not know their company's monitoring policies [52].

Eric Schmidt, chief information officer at Bricker & Eckler, suggests that monitoring policies be clearly defined and distributed to all employees through a wide variety of communication channels. The channels can be via letter, phone, fax, e-mail, Internet, Intranet, and a host of other media. The timing of the communication can be important. Recruitment, training, and orientation programs should have some mention of the monitoring policy. Face-to-face meetings between managers and staff could help clarify the seriousness of the policy and allow questions and answers to be provided. These face-to-face meetings also could have illustrations of what would be an example of clear misuse of the standards [7]. The same can be said for location monitoring.

Discipline. Discipline research focuses on the need for employees to receive warnings for infractions of company policy [26] [58]. Warnings are a part of progressive discipline widely used in corporations and supported by discipline research and texts e.g., [26] [58] [22]. Warnings are part of the "hot stove rule" that suggests employers (and hot stoves) clearly communicate dangers in violating rules (or getting near a hot stove). The ratings also appear to support those who recommend that clear warnings should be given to employees about surveillance activities e.g., [15] [7] [2] [30] [57] [9].

It is possible that most employees would be fired if everything they did were searched or investigated. Employers need to provide flexibility in deciding what violations would be worthy of immediate dismissal versus just an oral warning. Employers should at least provide minimal guidelines on technology use or go into great detail on specific incorrect activities and consequences [4].

Impact of Location Monitoring Procedures. Typically top management is responsible for analyzing major employee handbook-related policies [31]. Various measures of impact can be analyzed by top management. Management could analyze employee reaction to location monitoring. Reactions could be in terms of job satisfaction, location monitoring satisfaction, employee trust, perceived communication levels, etc. The most difficult types of measures to analyze but perhaps the most valuable measures to obtain would be the effect of

location monitoring on the bottom line and overall company performance.

5.1 Limitations to published location monitoring policies

Though location monitoring policies published in handbooks, disseminated on the Intranet and Internet, or distributed via letter can clarify major legal and ethical problems associated with the policies, the documents themselves have significant limitations. For example, employee handbooks can be changed at the employer's will at any time. Handbooks customarily state that they are not employment contracts. Respondents might not consider handbooks to be reliable or valid for their work to have a major effect on their perceptions of workplace policies. Second, employee handbooks are often not read by employees and supervisors. Handbooks typically are read most often when there is a crisis [31] [6]. Third, daily supervisory actions might hold more weight than employee handbooks that might be read (if ever) only during orientation periods. Fourth, technology use statements might be made by organizations but not enforced.

Employee handbooks are often developed to keep employers out of court [6]. Though many authors have recommended that handbooks contain clear technology use policies e.g., [7] [15], legal recommendations and ethical perceptions might not be highly related in some instances.

6. Suggestions for future research

Several new avenues of legal and ethical research should be undertaken to enhance discussion of location monitoring policies. The present study used a wide variety of keywords (e.g., employee, location, and monitor) in search engines and library databases to find legal and ethical literature on location monitoring and computer monitoring in general. One of the limits of such searches is English-based analysis. Other countries may have significant non-English texts covering location monitoring court cases relating to privacy, civil rights, and various security laws.

More detailed case analyses can be done within American courts. The National Workrights Institute [38] has summarized numerous court cases associated with the invasion of privacy and is collecting more Electronic Communications Privacy Act cases. Their conclusions were reported earlier.

Survey research can help analyze management and employee attitudes toward the need for and ethics of location monitoring. In related e-mail monitoring research, about 68 percent of employers that monitor employees cite legal liability as their primary reason [43]. Perhaps legal liability would also be a primary reason to monitor the location of employees.

Survey research also can help analyze how common various location monitoring policies are and what type of organizations would use location monitoring. A key question is whether employees should be notified about location monitoring in all instances. Various companies may have conflicting policies that reflect the conflicting recommendations shown in the literature. For example, Goodwin recommends using covert monitoring only when there is evidence that a crime has been committed [19]. The National Workrights Institute recommends avoiding any covert monitoring [38].

7. References

[1] G. S. Alder, "Ethical issues in electronic performance monitoring: a consideration of deontological and teleological perspectives," *Journal of Business Ethics*, vol. 17, pp. 729-744, 1998.

[2] AllBusiness, "Employee Records", 2001. http://www.allbusiness.com.

[3] American Civil Liberties Union, "Surveillance Under the USA Patriot Act", 2004, Available: http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12263&c=206.

[4] M. C. Attaway, "Privacy in the workplace on the Web," *Internal Auditor*, vol. 58, pp. 30-35, 2001.

[5] D. Banisar, *The Freedominfo.org Global Survey: Freedom of Information and Access to Government Record Laws Around the World,* May 2004. http://www.freedominfo.org/survey.htm.

[6] M. Baskin, "Is it time to revise your employee handbook?" *Legal Report*, Society for Human Resource Management, Alexandria, Virginia, Winter, 1998.

[7] S. Boehle, "They're watching you: workplace privacy is going, going…." *Training,* vol. 37, pp. 50-60, 2000.

[8] J. Bosch, "None of your business (interest): the argument for protecting all employee behavior with no business impact. *Southern California Law Review*, vol. 76, pp. 639-662, 2003.

[9] Bureau of National Affairs, *BNA Employment Guide*, Washington, D. C.: Bureau of National Affairs, 2004.

[10] L. L. Byars, L. L. and L. W. Rue, *Human Resource Management* (7th ed.), McGraw-Hill, Irwin, Boston, 2004.

[11] M. Camardella, "Electronic monitoring in the workplace". *Employee Relations Today*, vol. 30, pp. 91-100, 2003.

[12] M. Chan, "Corporate espionage and workplace trust/distrust". *Journal of Business Ethics*, 42, 43-58, 2003.

[13] D. J. Corry and K. E. Nutz, "Employee e-mail and Internet use: Canadian legal issues," *Journal of Labor Research*, vol. 24, pp. 233-257, 2003.

[14] S. Doherty, *Monitoring and Privacy: Is Your Head Still in the Sand?* 2001, http://www.nwc.com/1213/1213fl.html.

[15] EPolicy Institute (2001). *EPolicy Handbook*, 2001, www.epolicyinstitute.com.

[16] Federal Communications Commission. Fact Sheet: E911 Phase II Decisions, 2001, http://www.fcc.gov/Bureaus/Wireless/News_Releases/2001/nw10127a.pdf.

[17] B. Feldacker, *Labor Guide to Labor Law*, Prentice-Hall, Englewood Cliffs, N. J.: 1990.

[18] C. Forelle, "On the Road Again, But Now the Boss is Sitting Beside You," The Wall Street Journal (Eastern Edition), May 14, 2004, p. A.1.

[19] B. Goodwin, "Tell staff about e-mail snooping or face court, new code warns," *Computer Weekly*, vol. 38, p. 5, June 17, 2003.

[20] L. P. Hartman, "The rights and wrongs of workplace snooping," *Journal of Business Strategy*, vol. 19, pp. 16-20, 1998.

[21] S. R. Hawk, "The effects of computerized performance monitoring: an ethical perspective.," *Journal of Business Ethics*, vol. 13, pp. 949-958, 1994.

[22] W. H. Holley, K. M. Jennings, and R. S. Wolters *The Labor Relations Process*, (7th ed.), Southwestern, Mason, Ohio, 2001.

[23] G. James, "Can't hide your prying eyes," *Computerworld*, vol. 38, pp. 35-36, March 2004.

[24] G. E. Kaupins, "Ethical perceptions of corporate policies associated with employee computer humor." *Ethics and Critical Thinking Quarterly Review, vol. 2004, issue 1, pp. 16-35, 2004.*

[25] N. J. King, "Electronic monitoring to promote national security impacts workplace privacy," *Employee Responsibilities and Rights Journal*, vol. 15, pp. 127-147, 2003.

[26] T. L. Leap, & M. Crino, "How serious is serious," *HR Magazine*, vol. 44, pp. 43-48, 1998.

[27] Levijoki, Sami. Privacy vs Location Awareness. 2004. http://www.hut.fi/~slevijok/privacy_vs_locationawareness.htm.

[28] K. D. Loch, S. Conger, & E. Oz, "Ownership, privacy, and monitoring in the workplace: a debate on technology and ethics," *Journal of Business Ethics*, vol. 17, pp. 653-654, 1998.

[29] K. Martin, & R. E. Freeman, "Some problems with employee monitoring," *Journal of Business Ethics*, vol. 43, pp. 353-361, 2003.

[30] R. O. Mason, F. M. Mason, & M. J. Culnan, *Ethics of Information Management*, Sage Publications, Thousand Oaks, California, 1995.

[31] R. L. Mathis, and J. H. Jackson, Human Resource Management (10th ed.), Southwestern, Mason, Ohio, 2003.

[32] M. J. McCarthy, Keystroke cops: new software raises troubling questions on worker privacy, 2000. http://www.msnbs.com/news/3/8/00.asp.

[33] S. Miller, and J. Weckert, "Privacy, the workplace, and the Internet," *Journal of Business Ethics*, vol. 28, pp. 255-266, 2000.

[34] R. P. Minch, "Privacy Issues in Location-Aware Mobile Devices," *HICSS-37 Proceedings*, IEEE Press, 2004.

[35] "Location-Based Services." 2002. http://www.mobileinfo.com/locationbasedservices/market_outlook.htm on 5/21/04.

[36] A. D. Moore, Employee monitoring and computer technology: evaluative surveillance v. privacy. Business Ethics Quarterly, 10, 697-710, 2000.

[37] F. Morris, "The electronic platform: email and other privacy issues in the workplace," *Computer and Internet Lawyer*, vol. 20, pp. 1-9, 2003.

[38] National Workrights Institute, "Electronic Monitoring in the Workplace: Common Law and Federal Statutory Protection." 2004, Available: http://www.workrights.org/issue_electronic/em_common_law.html.

[39] D. R. Nolan, "Privacy and profitability in the technological workplace," *Journal of Labor Research*, vol. 24, pp. 207-232, 2003.

[40] Norwegian Parliament. "Act of 14, April 2000 No. 31 Relating to the Processing of Personal Data (Personal Data Act)." 2000. http://www.personvern.uio.no/regler/peol_engelsk.pdf.

[41] Organization for Economic Cooperation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 2000, OECD Publication Service, Paris. http://www1.oecd.org/publications/e-book/9302011E.pdf.

[42] A. J. Persson, & S. O. Hansson, "Privacy at work—ethical criteria," *Journal of Business Ethics*, vol. 42, pp. 59-70, 2003.

[43] W. G. Porter, and M. C. Griffaton, "Between the devil and the deep blue sea: monitoring the electronic workplace," *Defense Counsel Journal*, pp. 65-77, 2003.

[44] M. Prince, "Employers should establish clear rules on e-mail," *Business Insurance*, vol. 35, pp. 25-28, 2001.

[45] E. P. Robinson, "Update on employer e-mail monitoring: the Ninth Circuit joins the mainstream," *The Labor Lawyer*, vol. 18, pp. 355-363, 2003.

[46] Rossmore House, 269 NLRB 1176, 1984.

[47] A. Sharpe, & C. Russell, "Private rights and public policy," *Computer Law and Security Report*, vol. 19, pp. 411-415, 2003.

[48] Snekkenes, Einar. Concepts for Personal Location Privacy Policies. ACM: EC'01, Tampa Florida, October 2001, pp. 48-57.

[49] R. B. Standler, Privacy Law in the United States. http://www.rbs2.com/privacy.htm#anchor444444.

[50] State of Idaho Office of the Governor, *Executive Order 98-05: Establishing Statewide Policies on Computer, The Internet, and Electronic Mail Usage by State Employees*. 1998. http://ww2.state.id.us/gov/execord/EO98-05.htm.

[51] R. R. Sims *Ethics and Corporate Social Responsibility*, Praeger, Westport, Conn., 2003.

[52] S. Swanson, Beware: employee monitoring is on the rise. Informationweek, Issue 851, 57-58 August 20, 2001.

[53] S. Teicher, "It's 2 a.m. Do you know where your workers are?," The Christian Science Monitor, Dec. 22, 2003, p. 14.

[54] A. M. Townsend, & J. T. Bennett, "Privacy, technology, and conflict: emerging issues and action in workplace privacy," *Journal of Labor Research*, vol. 24, pp. 295-205, 2003.

[55] Location Privacy Protection Act of 2001. Accessed through title search at http://Thomas.loc.gov on 5/21/04.

[56] R. Want, "RFID, A key to automating everything," *Scientific American*, vol. 290, pp. 56-65, 2004.

[57] B. Venable, & H. Venable, *Workplace Labor Update* Venable, New York, July 1997.

[58] A. M. Zack, *Grievance Arbitration*, American Arbitration Association, New York, 1989.