Workplace E-Monitoring and Surveillance of Employees: Indirect Tool of Information Gathering

Ikonne Chinyere N[1], Prof. Ikonne Chiemela N[2]

[1]Ph.D, Department of Information Resources Management, Babcock University, Ilishan Remo, Ogun State, Nigeria

[2]Education Director, West-Central Africa Division of Seventh-day Adventist, Abidjan, Côte d'Ivoire

Abstract: ***This paper discussed how employers indirectly gather information on their employees in the workplace. The means used in achieving this aim is through e-monitoring and surveillance. Some forms and methods of e-monitoring and surveillance applications were indentified. Rationales in favor of and against e-monitoring and surveillance of employees were also reviewed. Employers argue that e-monitoring and surveillance are indispensible for the employees' effective performance and security of the organization. On the other hand, employees contend that workplace e-monitoring and surveillance is a system that infringe on their privacy. It was discovered that one of the ways by which this conflict could be resolved is by establishing a clear and balanced written policy regarding the implementation of e-monitoring and surveillance in the workplace. This should be a part of employee's work contract and might lead to the balancing of the rights of both the employers and employees to the workplace.***

Keywords: employee, workplace e-monitoring, electronic surveillance, information gathering, employee privacy right

1. Introduction

Workers around the world, in particular, in the more developed countries, are viewed to be frequently subjected to some kind of electronic monitoring and surveillance by their employers. As [1] have noted, for a long time, workplace monitoring has existed in one form or another. There is the tendency that it will continue to increase as technology advances, and will become increasingly sophisticated. Conversely, employees are not in favour of the use of e-monitoring and surveillance in that they opine that it intrudes in their right to privacy. Based on this, [2] states that surveillance techniques can be used to harass, discriminate, and to create unhealthy dynamics in the workplace.

Workplace electronic surveillance is a method through which organizations monitor the activities or gather data about their employees by using the tools and devices of Information Technology (IT), [3]. Office of Technology Assessment (cited in [4]) defines electronic monitoring as "the computerized collection, storage, analysis, and reporting of information about employees' productive activities" (p. 27). As discussed by Bhatt (in [5]), employee monitoring is in line with knowledge management in that organizations must create an environment of accountability and transparency that would enable them operate effectively. Electronic workplace monitoring could be used synonymously with work-place surveillance, [4]. According to [6], these technological activities offer managers the ability to map their employees' communication. In an attempt to observe, assess, and increase the performance and productivity of the employees, [7]; and to decrease abuses or waste, and control undesirable employee behaviors, [8], employers have created a whole new range of ways in which they can try to constantly watch on those they are supervising. So, instead of having to watch every person one at a time but not seeing everyone at the same time, employers have resolved to use some types of surveillance that could allow them watch all of their employees at all time and to be able to monitor the behavior and activities of the employees. Based on this, [8] and [9] posit that the diffusion of computers and information technology as well as electronic devices into organization has altered the relationship between employers and employees

With the increasing use of e-monitoring and surveillance of employees in the workplace, the concerns of employees and their reactions on their right to privacy have also been debated. The loss of control over personal information is perceived to be the most significant of all privacy issues. Employees opine that they are not able to determine when, how, and to what extent information about them is communicated to others. [10] asserts that electronic workplace monitoring and surveillance involve important negative privacy concerns in that it permits the employers to have access to employee's private communications such as e-mail and other Internet activities. As discussed by [11] employees are of the opinion that their non job-related communications are private and, consequently, should not be monitored by their employers.

The main purpose of this paper is to discuss some of the indirect tools through which employers gather information in the workplace. In addition, the paper will highlight the rationales in favor and against e-monitoring as well as employees' privacy right concerns.

2. Methods of Workplace E-Monitoring and Surveillance

[12] cite Botan who identifies workplace monitoring as a form of information gathering. Employers utilize different kinds of sophisticated software and hardware devices that can expose any action employees could have performed [5]. Some of the methods that have been incorporated to assist in workplace monitoring of employees include electronic monitoring of email communications, website viewing,

computer keystroke capturing, listening in on phone calls, and video surveillance, [8].

E-mail communication and Internet scanning: According to Segarnick [in 13], the number of US organizations that monitor e-mail usage of their employees have increased. [14] point out that most medium and large companies use technology to intercept electronic mail messages and monitor an employee's use of the phone, internet, access private conversations, other private communications and interactions. As has been observed by [15], a stored e-mail can provide records of communications that can be legally retrieved and printed for review. Employers argue that the monitoring of Internet activities is related to loss of productivity, degradation of available IT resources, and the high risk of liability [16].

Telephone tapping or recording: [15] and [14] remark that employers are involved in the official and unofficial tapping of the telephone lines of employees to collect information. Employers make us of telephone tapping so as to prevent personal use of telephones, [3]. They also check calls to confidential help lines. This is done by programming computers to count the number and type of calls and call-backs, the number of messages opened and waiting, the precise duration of each call, and the time period between calls [9].

Data Entry Monitoring: Computers are programmed to monitor the number of drafts of computer documents and the number of revisions per line of dictation and computer keystroke capturing, [9], [8]. The goal is to automatically count every key stroke of data-entry and data-processing clerks. Computers can also be programmed to monitor clerical workers thereby recording the number of key strokes per minute, the precise time and location of any errors. Data entry monitoring may also give information on the amount of time it takes to process or complete each task. [5] points out that keystroke monitoring is probably one of the most invasive types of monitoring.

Network Surveillance: As described by [15], managers use network surveillance to find out if employer-owned computers and Internet services are being used by employees to facilitate online shopping and to access pornography or other questionable sites. Employers use electronic surveillance to monitor any or all employee messages and even their physical behaviors.

Biometric surveillance: Biometrics is a term that applies to the many ways in which human beings can be identified by unique aspects of the body, [17]. Biometric surveillance provides information that measures and analyzes human physical and/or behavioral characteristics for authentication, identification, or screening purposes. The most commonly known biometric identifier example is the fingerprints.

3. Rationale in favor of Employee E-Monitoring and Surveillance

Employee's electronic monitoring and surveillance have raised concerns from all areas of society – business organizations, employee interest groups, privacy advocates, civil libertarians, lawyers, professional ethicists, and every combination possible. [18] say that the rate at which organizations have engaged in the monitoring of workers has been increasing at least for the past ten years. As have been reported by [19], the AMA survey of 2005 reveals that seventy six percent (76%) of organizations are engaged in tracking their employees' Internet usage. In the view of [15], the survey of American Management Association's (AMA) of 2001 workplace monitoring and surveillance reveals that eighty-two percent (82%) of the managers who responded to their survey used some type of electronic monitoring in the workplace. Further, [20] narrate that the AMA survey of 2003 reveals that out of 526 companies representing a wide range of sizes and types, more than 75% of the companies monitor employees' web site connections. Half of these corporations use video surveillance primarily to guard against theft and sabotage. According to [18], the Center for Business Ethics asserts that as high as ninety-two percent (92%) of all organizations electronically monitor and track their employees in some form or another. In spite of the fact that there are employees' concerns and some setbacks regarding workplace electronic monitoring, these findings show that e-monitoring and surveillance are actually on the increase. Should organizations have the right to monitor employee communications? Below are some of the major reasons that precipitate monitoring of employees at work.

Employee Productivity: According to [21], workplace monitoring can be beneficial for an organization to obtain productivity and efficiency from its employees. Organizations that argue in favor of monitoring see it as a form of productivity and security tool [9]. Employers claim that surfing the Internet and sending personal e-mails take up much time and consequently this reduces productivity. They argue that every minute spent in surfing the internet is not spent in increasing revenue. For instance, [22] report that there is potential annual productivity loses which could amount to one million dollars a year. Therefore, to enhance and increase productivity and to discourage surfing of the internet, most of the employers consider it necessary to institutionalize systematic and continuous scrutinizing in the workplace through electronic surveillance system, [3].

Security Concerns: Employers feel increasingly susceptible to security concerns. They reason that most security breaches come from employees with deep knowledge of organizational operations. Employers opine that employees could e-mail their trade secrets, designs, formulas, confidential documents, as well as their intellectual property rights quickly and easily to a large audience during their communication, [23], [3], [24]. So by monitoring Internet usage and content, organizations argue that they are able to detect and halt security breaches. In addition, they argue that the mere knowledge of increased surveillance may deter potential employee theft. Therefore, safeguarding and the confidentiality of their information motivate employers in the utilization of electronic monitoring technology.

Further, employers claim that they have an absolute right to protect themselves and their property from security risks created by employment. Employers, according to [25], posit that company procedures, management supervision and the presence of security staff, are not enough to resolve these security threats. Based on this, Ham (in [26]) asserts that employers justify the introduction of surveillance tools so as to minimize “the risk of theft, protect the premises from threats to property such as sabotage, arson and vandalism and reduce the risk of extortion by employees.”

Workplace Liability Risks and Investigations: Potential legal liabilities resulting from employees’ computer misuse or misconduct is often a motive for employee monitoring. Employers wish to protect themselves from liability associated with misuse of employer-owned Internet and e-mail resources. In addition, incidents of harassment, safety and theft may trigger an investigation into such misconduct that may use monitoring or surveillance, [27]. Therefore, employers justify workplace surveillance as a way of reducing exposure to liability risks.

Employee or Customer Safety: According to [28], issues such as increasing attacks, robberies, violence, workplace mishaps, other workplace safety issues as well as other matters that are associated with liabilities and damages have motivated employers to monitor the workplace. Employers point out that they have an absolute right to protect themselves and their property from security risks created by employment. So, electronic monitoring and surveillance are mechanisms put in place to prevent criminal activities in the workplace, [3]

Network and Systems Performance: Another major concern of employers is network bandwidth traffic which includes slowdowns that are related to employees downloading, sharing and using large audio and video files, Internet surfing and high volumes of personal e-mail. These activities can also introduce viruses that may attack and disable a network. [3] also note that it as a measure in preventing workplace inefficiencies, malware, data loss and viruses as the main threats caused by insecure use of Web 2.0 applications like social networking, blogs and wikis.

4. Rationale against employee e-monitoring and surveillance

As regards rationale against workplace monitoring and surveillance as well as its usage in the workplace, many people and organizations are against the e-monitoring activities of workers in the work place. This subject has also become a controversial subject because of the psychological and emotional cost that employees pay from being constantly monitored and surveilled, [8]. Employers have a legitimate interest in monitoring work to ensure efficiency and productivity, but it has been argued that e-surveillance often goes well beyond legitimate management concerns and becomes a tool for spying on employees. Employees do not want intrusive monitoring techniques used throughout the workday. Thus, the activity of workplace monitoring could be seen to present a classic conflict of interest between employers and employees. Below are arguments or the essential conflicts of workplace monitoring.

For one, monitoring an employee borders on a possible invasion of that employee’s personal privacy and this is the greatest concern of the advocates. [10, p. 381] states that “Privacy is the exclusive right to dispose of access to one’s proper (private) domain.” [29] and [30] have acknowledged that electronic surveillance threatens employee privacy and according to [3], this leads to intrusion and invasion of their privacy and dignity. This invasion of privacy can literally make employees sick, which may also have a counter effect on the productivity that organizations seek.

Next, it is believed that electronic monitoring and surveillance lead to increased pressure on employees to meet performance levels. As have been noted by [31], this could defeat the major purpose of monitoring which is to increase productivity and efficiency in the workplace. A major criticism of e-monitoring is that increased pressure to meet performance could increase levels of stress, decrease job satisfaction and work life quality. Also, it could lead to lower morale and resentment, and, subsequently, creating suspicion and tension between the employers and employee. [32] observes that studies have shown that there is a link between monitoring and psychological and physical health problems, increased boredom, high tension, extreme anxiety, depression, anger, severe fatigue, and musculoskeletal problems. More, [3] affirm that since employees feel that every action of theirs is continuously monitored, the stress that results from this could result in health issues such as an increased blood pressure. It has been noted that people under stress are sick more often and heal more slowly; the resultant cost is an increase in sick leave and a decrease in productivity. Therefore, this pressure and hostility in the workplace could lead to a decline on the productivity level of the organization.

Further, e-surveillance can strain and damage the employment relationship as well as the mutual trust that exist between an employee and his employer [3], [33]. E-monitoring could also inject suspicion and hostility in the workplace which may, in turn, lead to employee resentment and might eventually lead to counter-productive behavior. Finally, according to NSW Young Lawyers [34], workplace surveillance data has the potential to be abused by the employer. For instance, employees could commit some kind of violation whilst using employer’s computer or internet communications in their work. If an employer uses this data incorrectly, it can serve as an incentive for discrimination, unfair dismissal and other abuses.

5. Solution to workplace e-monitoring and surveillance and employees’ privacy conflict

One of the major arguments regarding workplace e-surveillance and monitoring is that such surveillance infringes on employees’ rights to privacy. Employers reason that they need to protect their organization from employee activities, arguing that this protection outweighs employees’ quest for privacy in the workplace. But some authors like [14], [29], [30], [35], [36] contend that the right to privacy is more important than an organization’s right to efficiency and profitability. They posit that employees are entitled to some forms of privacy as well as relaxation and not having to be continuously monitored by managers.

When an employee is at work, the right to privacy is either nonexistent, or significantly less than the one enjoyed after work hours, [5]. In view of this, there must be a solution that could accommodate the needs of both the employers and employees.

A part of this solution could be to balance the needs of the employers and employees regarding workplace e-surveillance and monitoring conflict. Balancing the legitimate needs of both the employers and employees is not insurmountable. This could be achieved when organizations inform employees of the purpose of monitoring activities, set privacy expectations, and create reasonable monitoring policies. As have been expressed by [28], [15], and [37], one of the reasonable courses of action would be to have a monitoring policy and follow it. Acceptable "Use Policies" according to [5], are one of the most common company policies that outline the approach on how employees can use company systems and what they can expect as privacy.

[38] add that by establishing clear-cut policies, this will set boundaries, establish employees' expectations of privacy, and help set a workplace tone that conveys organizational responsibility and respect for others. The policy should apply to all employees including all levels of the organization and the reasons for the policy should be clearly explained. [39] and [40] further posit that organizations' policies should be in writing and placed in appropriate company employee manuals and literature. This is to ensure that workplace surveillance does not result in discrimination, abuse or an invasion of privacy. In addition, Duermyer (in [5]) assert that the policy should be audited by the organizations at least annually to determine if it is in step with current procedures.

Another recommendation according to Lindquist (in [13]), is the establishment of employees' trust and the proper training of employees before implementing e-monitoring technologies. Further, Segarnick (in [3]) suggests that employers should ensure that any e-surveillance or monitoring activity is conducted fairly and transparently. In so doing, the legitimate interests and rights of both the employers and employees will be protected. More, employers must be careful when monitoring, not to violate labor or anti-discrimination laws by targeting specific employees. Finally, the assertions of [3], [28] and [26] are that if possible, surveillance should not extend to performance monitoring or personal information gathering. However, in case it is done, it should only be conducted with the prior knowledge or preferably consent of those to be monitored.

6. Conclusion

This paper has reviewed some of the issues concerning workplace e-monitoring and surveillance. It was revealed that workplace e-monitoring and surveillance is controversial as it causes conflicts and dilemmas between employers and employees. This is mainly due to the fact that employers see this mechanism as their means of improving work performance, efficiency and security, while employees perceive it as an intrusion into their privacy. Apparently, workplace employee e-monitoring and surveillance have come to stay as long as organizations wish to increase their productivity and protect their companies from security concerns. And at same time, employees will always advocate for their rights for privacy in the workplace. In view of this conflict, employers should endeavor to strike a balance between their right to run their companies' business productively and efficiently and, at the same time, grant employees their reasonable rights to privacy. In addition, employers should train and educate their employees; preferably, before the implementation of e-monitoring and surveillance systems in the workplace to ensure that employees understand how these Information Technologies (IT) function. Further, employers should have a monitoring policy as a part of their work contract which is to be given to each employee who, in writing, acknowledges receipt thereof. They should also clearly set out permitted and prohibited uses for e-mail, internet and applications and other areas that could be monitored whilst in the office. Finally, in the case of the actual e-monitoring, employers should be fair, transparent, and should avoid gathering personal information of their employees.

References

[1] G. D. Nord and T. F. McCubbins, "E-monitoring in the workplace: Privacy, Legislation and Surveillance Software," *Communications of the ACM*, vol. 49, no. 8, 2006.

[2] EPIC --- Privacy and Human Rights Report (2006) [Online] Available:http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Workplac.html#fnB303 (October 16, 2014)

[3] A. M. Sheriff and G. Ravishankar, "The techniques and rationale of e-surveillance practices in organizations," *International Journal of Multidisciplinary Research*, vol. 2, no. 2, 2012.

[4] J. M. Mishra and S. M. Crampton, "Employee monitoring: Privacy in the workplace? *Advanced Management Journal*, vol. 63, no. 3, 1998.

[5] J. Yerby, "Legal and ethical issues of employee monitoring," *Online Journal of Applied Knowledge Management*, vol. 1, no. 2, pp. 44-55, 2013

[6] C. D'Urso, "Who's watching us at work? Toward a structural-perceptual model of electronic monitoring and surveillance in organizations," *Communication Theory*, vol.16, pp. 281-303, 2006.

[7] B. P. Kane, "Monitoring employee e-mail usage. *Advocate (Idaho)*, vol. 44, p. 20, 2001.

[8] S. Coultrup and P. D. Fountain, "Effects of electronic monitoring and surveillance and the psychological contract of employees: An Exploratory study proceeding of ASBBS, *Annual Conference*: Las Vegas, vol. 9, no. 1, 2012.

[9] L. C. Hébert, "Methods and extent of employer use of electronic monitoring and Surveillance, *Employee Privacy Law*, 1, Section 8A: vol. 1, 2002.

[10] L. E. Rothstein, "Privacy or dignity: Electronic monitoring in the workplace," *New York. Law Journal of International and Comparative Law*, vol. 9, p. 379, 2000.

[11] A. Rogers, “You got mail but your employer does too: Electronic communication and privacy in the 21st century workplace,” *Journal of Technology Law and Policy*, vol. 5, p. 1, 2002.

[12] Vorvoreanu, M. and Butan, C. H., *Examining electronic surveillance in the workplace A review of theoretical perspectives and research findings*, CERIAS *Tech Report*, 2001[Online] Available: *https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2001-32.pdf* (October 10, 2014)

[13] Cox, S., Goetter, T., & Young, D. *Workplace Surveillance and Employee: Implementing an Effective Computer Use Policy Communications of the IIMA*, vol. 59, no. 5, 2005, [Online] Available: http://www.iima.org/CIIMA/CIIMA%205.2%2057%20Cox-6.pdf (April 15, 2014)

[14] S. Miller and J. Weckert, “Privacy, the workplace and the Internet. *Journal of Business Ethic*, vol. 28, pp. 255-265, 2000.

[15] Wakefeild, R. L. Employee monitoring and surveillance—The Growing Trend. *Information System Control Journal*, vol.1, 2004. [Online] Available:https://www.google.ci/search?q=Wakefeild,+R.+L.+(2004).+Employee+monitoring+and+surveillance&ie=utf-8&oe=utf-8 (April 21, 2014)

[16] V. Lim, “The IT way of loafing on the Job Cyberloafing, neutralizing and Organizational justice, *Journal of Organizational Behavior, vol.*23, pp. 675-694, 2002.

[17] M. Nieto, K. Johnson-Dodds, and C. W. Simmons, “Public *and Private Applications of video surveillance and biometric technologies*, Sacramento: California Research Bureau, 2002.

[18] N. Firoz, R. Taghi, and J. Souckova, “E-mails in the Workplace: The Electronic Equivalent of ‘DNA’ Evidence,” *Journal of American Academy of Business*, vol. 8, no. 2, pp. 71-78, 2006.

[19] C. DePree and R. Jude, “Who’s Reading Your Office Email? Is That Legal? *Strategic Finance*, vol. 87, no. 10, pp. 44-47, 2006

[20] M. W. Allen, K. L. Walker, S. J. Coopman, and J. L. Hart, “Workplace Surveillance and Managing Privacy Boundaries, *Management Communication Quarterly*, vol. 21, no 2, pp. 172-200, 2007.

[21] P. J. Bezek and S. M. Britton, “Employer monitoring of employee internet use and e-mail,” *MEALEY’S Cyber Tech Litigation*, Report, 2, 2001.

[22] Z. Court and C. Warmington, “The workplace privacy myth: why electronic monitoring is here to stay, *Employment and Labor Law*, vol. 29, no. 1, pp. 1-20, 2004.

[23] M. Oprea “An agent-based knowledge management system for university research activity monitoring, *Informatic Economica*, vol. 16, no 3, pp.136-147, 2012.

[24] Schulman, A. (2001). The Extent of Systematic Monitoring of Employee E-mail and Internet Use, [Online] Available: http://www.sonic.net/~undoc/extent.htm (February, 19, 2014)

[25] D. Long, “Documenting Employee Discipline” Council on Education in Management, Discipline and Termination Law, *Thomspon Law*, 1999.

[26] Cripps, A. (2004). Workplace Surveillance, New South Wales Council for Civil liberties. [Online] Available: http://wenku.baidu.com/view/3b1fd16e1eb91a37f1115c65.html (January 30, 2012)

[27] T. Bromberg,). “Investigating Employee Misconduct in the age of Privacy Law,” *Journal of Workplace Trend*, 2004.

[28] C. McHardy, T. Giesbrecht, and P. Brady, “Workplace Monitoring and Surveillance. *McCarthy Tétrault* LLP, 2005.

[29] P. Findlay and A. McKinlay, A. “Surveillance, electronic communications technology and regulation,” *Industrial Relations Journal*, vol. 34, pp. 305-318, 2003.

[30] F. Lane, “The naked employee: How technology is compromising workplace privacy, New York: *American Management Association*, 2003.

[31] N. Watson, “The private workplace and the proposed “Notice of Electronic Monitoring Act”: Is “Notice” Enough. *Federal Communication law Journal*, vol. 54, no. 1, pp. 79-104, 2001.

[32] L. P. Hartman, “The Rights and Wrongs of Workplace Snooping,” *Journal of Business Strategy, vol.* 19, no. 3, vol.16, no. 4, 1998.

[33] T. Dixon, “Invisible Eyes: Report on Video Surveillance in the Workplace,” *The Privacy Committee of New South Wales*, *Report*, 67, 1995.

[34] NSW Young Lawyers, “Submissions on Workplace Surveillance Bill 2004”, *Employment and Industrial Law Committee*, 2004.

[35] C. Hardy and S. Clegg, “*Some dare call it power*. In S. Clegg, C. Hardy, & W. Nord (Eds.), *Handbook of organization studies*, London: Sage, pp. 622-641, 1996.

[36] P. Thompson, “Fantasy island: A Labour process critique of the “age of Surveillance,” *Surveillance and Society*, vol. 1, no. 2, pp.138-151, 2003.

[37] K. Kovach, J. Jordon, K. Tansey and E. Framinan, “The Balance Between Employee Privacy and Employer Interests,” Business *and Society Review*, *vol.* 2, pp. 289-298, 2000.

[38] H. Adams, S. M. and S. A. Feeley, “E-mail Monitoring in the Workplace: The Good, the Bad and the Ugly,” *Defense Counsel Journal*, vol. 67, no. 1, *International Association of Defense Counsel.* 2000.

[39] J. Totten, “*The Misuse of Employer Technology by Employees to Commit Criminal Acts,”*ABA Section of Labor and Employment Law Technology Committee Midyear Meeting, Miami, Fl., 2004.

[40] F. Morris, “The Electronic Platform: Email and Other Privacy Issues in the Workplace,” *Computer and Internet Lawyer*, vol. 20, pp. 1-9, 2003