Employee Opinion about Ethical Dimensions of E-Monitoring in MNCS in Dubai

Sangeetha Vinod*
Fayaz Ahamed**

THE internet, e-mail and instant messaging have become essential tools that staff uses to communi-cate, collaborate and carry out research. Wikis, weblogs, forums, social-networking websites, and instant messaging are no longer strictly leisure time technologies – they have become vital
business resources used in marketing, research, and communication. But they are resources which can also be misused or abused.

How much time does your employee spend surfing the internet ("cyber slacking")? Lost productivity is not the only computer-related risk that organizations face. The improper use of e-mail and instant messages can lead to extremely expensive lawsuits, and the proliferation of mobile devices has made it considerably easier for errant employees to steal sensitive information.

The purpose of this study is to understand about the ethical dimensions of electronic surveillance/monitoring (E-monitoring) of 30 employees from 3 Multinational Companies (MNCs) in Dubai, United Arab Emirates. The findings of the study highlighted that 73 percent of the employees strongly agreed that it is ethical for a superior to record, with notice; an employee's business related telephone calls, at the same time around 67 percent of them considered it highly unethical to the secret/with notice monitoring of emails. 77 per cent of the employees strongly agreed that electronic monitoring of an employee's work related activities should be done occasionally rather than on a continuous basis. 80 per cent of them considered secret monitoring by the employer as an unethical act that reduced their trust and commitment towards the management.

Key Words: *Employee monitoring (E-monitoring), Electronic surveillance, Cyber slacking, AUP - Acceptable Use Policy, ePolicy.*

Introduction

Employers want to be sure that their employees are doing a good job, but employees do not want their every sneeze or trip to the water cooler logged. That is the essential conflict of workplace monitoring. New technologies make it possible for employers to monitor many aspects of their employees' jobs, especially on telephones, computer terminals, through electronic and voice mail, and when employees are using the Internet. Such monitoring is virtually unregulated.

One company offers technology that claims to provide insight into individual employee behavior based on the trail of "digital footprints" created each day in the workplace. This behavioral modeling technology can piece together all of these electronic records to provide behavior patterns that employers may utilize to evaluate employee performance and conduct. For example, it might look for word patterns, changes in language or style, and communication patterns between individuals.

Objectives of the Study

The primary objective of the study is to understand the employee's opinion about E-monitoring by employers in select institutions in Dubai, United Arab Emirates. Is it an ethical or unethical act? This research question has a central focus in this research paper,

the responses of which will enable the researcher to give certain specific concluding remarks on the same.

Review of Literature

Electronic monitoring can be defined as the observing or listening to persons, places, or activities – usually in a secretive or unobtrusive manner – with the aid of electronic devices such as cameras, microphones, tape recorders, or wire taps. Therefore, unless company policy specifically states otherwise, your employer may listen, watch and read most of your workplace communications *(http://legal-dictonary.thefreedictionary.com)*.

A 2007 survey by the American Management Association and the ePolicy Institute, compiled in the ePolicy Handbook (Flynn, 2007), found that two-thirds of employers monitor their employees' web site visits in order to prevent inappropriate surfing. And 65 percent use software to block connections to web sites deemed off limits for employees. This is a 27 percent increase since 2001 when the survey was first conducted. Employers are concerned about employees visiting adult sites with sexual content, as well as games, social networking, entertainment, shopping and auctions, sports, and external blogs. Of the 43 percent of companies that monitor e-mail, nearly three-fourths use technology to automatically monitor e-mail. And 28 percent of employers have fired workers for e-mail misuse.

Close to half of employers track content, keystrokes, and time spent at the keyboard. And 12 percent monitor blogs to see what is being written about the company. Another 10 percent monitor social networking sites.

Almost half of the companies use video monitoring to counter theft, violence and sabotage. Of those, only 7 percent state they use video surveillance to track employees' on-the-job performance. Most employers notify employees of anti-theft video surveillance (78 percent), and performance-related video monitoring (89 percent).

The researchers will now describe the different techniques of e-monitoring carried out over the years, and currently by employers especially the MNCs as compiled in the Fact Sheet Seven, titled – Workplace Privacy and Employee Monitoring, Empowering Consumers, Protecting Privacy *(http://www.privacyrights.org/ar/Privacy-IssuesList.htm)*. They are as follows:

Telephone Monitoring

Employers may monitor calls with clients or customers for reasons of quality control. Telephone numbers dialed from phone extensions can be recorded by a device called a pen register. It allows the employer to see a list of phone numbers dialed by your extension and the length of each call. This information may be used to evaluate the amount of time spent by employees with clients.

Employers often use pen registers to monitor employees with jobs in which telephones are used extensively. Frequently, employees are concerned that the information gathered from the pen register is unfairly used to evaluate their efficiency with clients without consideration of the quality of service.

The best way to ensure the privacy of your personal calls made at work is to use your own mobile phone, or a separate phone designated by your employer for personal calls.

Company Cell Phones

Incoming and outgoing calls on company cell phones are likely to be monitored as well as text messages being exchanged. Employees who use their company owned cell phones have a high chance of being snooped upon. However, since the actual content of messages

are kept by the cell phone companies, the business may not want to pay extra to receive those reports.

Instant Messaging (IM)
Nowadays technology has progressed and the capability to monitor instant messages is available. According to Flynn (2005), ePolicy Institute Survey, only 10 percent of companies tracked their employees' instant messages. However, as IMs have become more pervasive, more companies are investing in tracking software for IM monitoring.

Social Networking
Social networking is a whole other ballgame. While employers can easily monitor and/or block websites that are accessed from work terminals, in addition many employers take it a step further and regularly surf the Internet to find out the scoop on their employees. Activities and messages posted on social networking sites are often found by employers which can lead to career disaster. Your boss can monitor your Facebook account, even if you restrict public viewing. If you access your favorite social media profiles on your work computer, you give your employer instant access to your entire profile. In fact, a recent study reveals that more than 70 percent of corporations have access to employees' use of social media.

There is a lot of controversy as to whether or not employers have the right to do this or if it is even ethical, but the bottom line is this kind of probing is not against the law, and anything is fair game on the Internet. As long as this remains to be, the reality is employers will continue to monitor social networks,

Computer Monitoring
If you have a computer terminal at your job, it may be your employer's window into your workspace. There are several types of computer monitoring.

- Employers can monitor Internet usage such as web-surfing and electronic mail. People involved in intensive word-processing and data entry jobs may be subject to keystroke monitoring. It also may inform employees if they are above or below the standard number of keystrokes expected.
- Another computer monitoring technique allows employers to keep track of the amount of time an employee spends away from the computer or idle time at the terminal.

Your employer can access your personal photos, videos, music, and more. Do you ever charge your phone or camera through your work computer? According to Jeffrey Keener, senior security engineer at Guidance, a company that produces company security software, "If you had an iPod or a digital camera charging through the USB port, we could browse all the files that were stored on the device."

Electronic Mail and Voice Mail
According to some reports, almost three-fourths of employers regularly track e-mail through technology, but 40 percent have an employee who is designated to peruse employee e-mail. Logging in to personal e-mail accounts from service providers such as Hotmail, Gmail, AOL or Yahoo! are accessed through company owned and run network connections.

If an electronic mail (e-mail) system is used at a company, the employer owns it and is allowed to review its contents. Messages sent within the company as well as those that are sent from your terminal to another company or from another company to you can be subject to monitoring by your employer. The same holds true for voice mail systems. In

general, employees should not assume that these activities are not being monitored and are private. If you do not want your employers to know what you are sharing in e-mail with contacts, it is probably best to not engage in personal e-mail during work hours using company equipment since monitoring goes for both company owned accounts and personal accounts.

Video Monitoring

For years now many businesses have installed closed-circuit TV systems to monitor the workplace, both during and after hours. Video monitoring is a commonplace method of deterring theft, maintaining security and monitoring employees. For example, a bank may utilize video monitoring to prevent or collect evidence on a robbery. A company may also use video monitoring in a parking garage as a security measure for employee safety.

Employers may also use cameras to monitor employee productivity and prevent internal theft. Many employers are now requiring smart cards which have computerized chips. Employee ID "key badges" help employers track where you have been, security software can track how long you spend away from your computer, and the GPS program on your company-issued cell phone can provide your exact location at all times. These cards are necessary for employees to enter and exit buildings, computer terminals, and other job related accesses.

Privacy in general has become a prominent issue, but in today's world it is pretty much a given to assume that privacy in the workplace is non-existent. Many companies offer technology policies to let employees know how and what is being monitored, but this is not always the case.

The researchers would like to highlight that one or more of these techniques the MNCs regularly apply on their employees, and based on the nature of work, attitude of management and Information Technology resources available in the organization, the techniques may also vary at different occasions. Now, let us see the rationale behind e-monitoring (especially the activities on computer) by employers.

Why you need to Monitor your Employee's Computer Activities?

Majority of employers monitor employee arrival times, cash handling, and the accuracy and quality of employees work. Monitoring in this manner is accepted as a business necessity and most organizations would consider it completely irrational not to make such checks. Yet, a surprisingly large number of organizations still do not adequately monitor the manner in which employees use their computers – and that can be an extremely costly omission. The misuse and abuse of computer equipment can have serious consequences for an organization like the following:

Lost Productivity

Personal surfing has become an enormous problem for employers. Estimates as to the amount of time that is lost to cyber slacking vary enormously, but most studies put it in the region of 2.5 hours per employee, per day. Multiply that 2.5 hours by the number of employees and the average hourly pay rate in your organization, and you will have a ballpark estimate of the cost of cyber slacking.

Intellectual Property Theft

Intellectual property theft (IPT) has always been a concern for companies – and internet-connected computers and mobile devices provide new opportunities for people to access and steal data. Documents and data can easily and speedily be transferred to a flash drive or laptop. Many organizations are concerned about outsider theft, but, in fact, the majority of thefts are committed by insiders.

Companies often do not admit to being victims of IPT, and so it is impossible to quantify the costs. The sums involved can, however, be considerable.

Fraudulent Activity

Employees often have access to sensitive personal information which can either be misused by the employee or sold on to a third party. HSBC customers had almost $500,000 stolen from their accounts after an HSBC employee passed on data to criminal associates (HSBC). The cost of fraudulent activity extends beyond the losses incurred as a direct result of the fraud – the financial effects of the damage to an organization's reputation and the loss of customer confidence can far outweigh the cost of the fraud itself.

Legal Liability

Many employers face lawsuits that result in the improper use of e-mail by employee – and such lawsuits can be extraordinarily expensive. Monitoring employee's computer activities is not a big brother tactic, it is a responsible business, and helps protect both an organization and its stakeholders – including its employees. Corporates can make use of different products available in the markets to name one, Effortz Solutions providers have launched software named as the Employee Activity Monitor – it is a powerful tool to monitor an employee's activity in real time with live key strokes, application usage details, monitor internet details, messenger conversations, emails' correspondence, desktop monitor screenshots and more.

Research Rationale and Methodology

Business executives have always monitored their employees' behavior. Electronic monitoring may be especially useful in training and improving productivity (Blylinsky, 1991; Laabs, 1992). However, critics of electronic monitoring suggest that the more obtrusive forms of electronic monitoring can lead to elevated levels of stress, decreased job satisfaction and quality of work, decreased levels of customer service, and poor quality (Kallman, 1993). Electronic monitoring, by imposing excess control over employee behavior, can alienate employees, and develop a feeling of working in a modern "sweetshop" (Kidwell and Bennett, 1994). Employers have the legal right to electronically monitor their employees (Kelly, 2001). The procedures for electronically monitoring employees must be designed with fairness and ethics in mind.

A number of studies have examined cross-cultural ethical business issues within the Chinese business environment. Roxas and Stoneback (2004), considered the issue of gender across cultures in ethical decision-making: a sample of junior and senior accounting students from eight countries was taken (U.S.A., Canada, Australia, China, Philippines, Thailand, Germany, and Ukraine). One interesting outcome of Roxas and Stoneback's study was that overall males were significantly less ethical than females; except in China where females are less likely to behave ethically. In anotherstudy, Redfern and Crawford (2004), sampled Chinese managers from the PRC (Peoples' Republic of China) and administered the Forsyth's (1980) Ethics Position Questionnaire with them. One result from their study indicate regional differences between Chinese managers: managers in South China scored different than managers in North China. In yet another study, Snell and Herndon examined the effective use of Code of Ethics by Hong Kong companies. From their research, it appears that cultural factors (power distance and traditional legalist assumptions) account for a gap between adopting Code of Ethics and adherence to them (Snell and Herndon, 2004). Wu (2004) studied business ethics operation between Taiwan and PRC enterprises. One observation made by Wu was the burden of the communist system in PRC as an obstacle to practicing sound ethical decisions for Chinese firms. In noting one last study, Douglas and Wier (2005), compared Chinese and U.S. managersconcerning cultural and ethical effects in budgeting systems. Douglas and Wier developed a model of cultural effects on budgeting

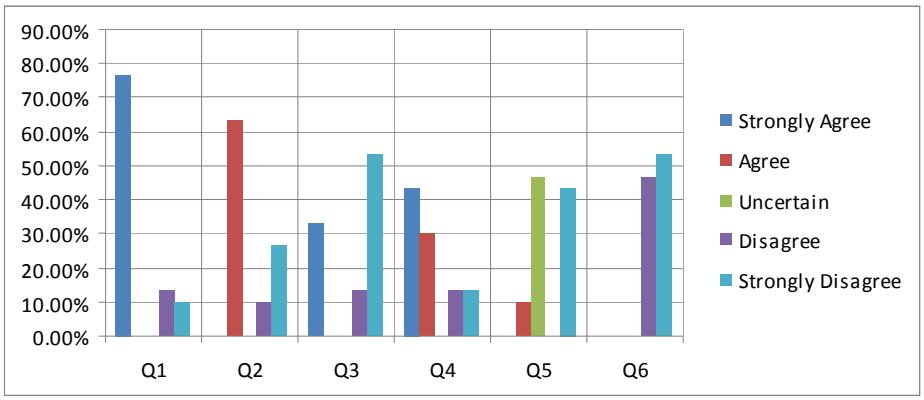
systems as influenced by culture-specific work-related and ethical values. The data from their study for the most part supported research model (Douglas and Wier, 2005). Therefore, the results of the study presented in this article adds to the above research by exploring the ethical dimensions of electronic monitoring of employees working in MNCs in Dubai, United Arab Emirates.

The questionnaire used in this study was based on one developed by Vaught, Taylor, and Vaught (2000) as presented in an article entitled, "The Attitudes of Managers Regarding the Electronic Monitoring of Employee Behavior: Procedural and Ethical Considerations".

The research design adopted is descriptive in nature, as it attempts to develop a profile of the executives from the MNCs, and their opinion on ethical dimensions of electronic monitoring. The primary data was collected by distributing questionnaires to 50 employees by Simple Random Sampling procedure in three Multinational companies (MNCs) in Dubai. The final sample size was 30 excluding the non-responses. The primary data was edited and tabulated using simple percentage analysis with the help of MS-Excel.

Results and Discussion

The 18 questions from the questionnaire have been divided into questions of six each, and illustrated through tables and graphs. The results will give a better understanding about the opinion of employees regarding electronic monitoring and whether they feel it is ethical or not.



Graph 1: Employee Opinion about Electronic Monitoring as an Ethical/Unethical Act.

Q. 1. The electronic monitoring of an employee's work related activities should be done occasionally rather than on a continuous basis.

Q. 2. Employees should be given notice (such as a blinking light on a telephone) each time they are being electronically monitored.

Q. 3. The secret video monitoring of an employee in his or her work area is ethical.

Q. 4. Giving employees written notice that they will be electronically monitored sometime in the future is adequate warning.

Q. 5. The collection of data, with notice, by a superior from an employee's computer for later review is ethical.

Q. 6. The simultaneous monitoring, with notice, by a superior of an employee's computer screen is ethical.

From the above analysis it is clear that 76.66 per cent of the employees strongly agreed that electronic monitoring of an employee's work related activities should be done occasionally rather than on a continuous basis. This indicates that the employees do believe that electronic monitoring is vital, and required to a certain extend in every organization. They do consider it ethical enough, as long as management does not resort to secret mechanism in surveillance.

Around 23 per cent of the employees either disagreed or strongly disagreed to the same perspective, and were of the opinion that if the organization conducts electronic monitoring even occasionally, it is still an unethical act that brings down their morale and level of commitment towards the organization.

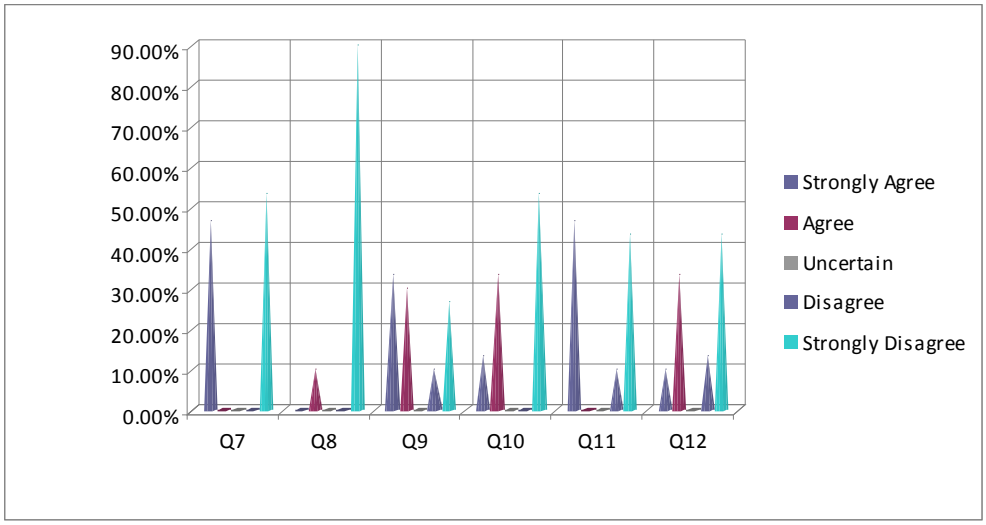
63 percent of the employees agreed to the statement that they should be given some sort of indication (like blinking of telephone) to be informed that they are being monitored, but 37 percent disagreed and strongly disagreed that this act of giving a cue is also unethical and un-warranted.

Around 67 percent of the employees strongly disagreed to the idea of secretly video monitored, and considered it as an extreme unethical practice. They claimed that as such they were videotaped at their work station and lobbies through the CCTV cameras, and a secret monitoring would create an unhealthy work environment wherein everybody has to put on a mask and not be their usual self, which they believe will affect their performance at work.

73 percent of the employees were of the opinion that they considered it ethical enough of being informed in written by the management about being electronically monitored, while 26 percent disagreed on the same and considered this as unethical enough, whether they were informed or not informed.

76 percent of the employees were uncertain about their feelings towards the concept of their superior collecting data with notice from their computers for later review as ethical. 43 percent strongly disagreed to the same and claimed this would create a conflicting relationship that will further affect the delegation and implementation of operational and strategic issues at work.

Simultaneous monitoring, with notice, by a superior of an employee's computer screen is ethical, this is one statement all the employees in one voice strongly disagreed too, and claimed that they would be very dissatisfied with such a situation and would eventually prepare to leave an organization that has such kind of practices.



Graph 2: Employee Opinion on the Different Techniques of Electronic Monitoring.

Q.7. The secret simultaneous monitoring by a superior of an employee's emails is ethical.

Q. 8. It is ethical for a superior to listen-in, with notice, on an employee's business related telephone calls.

Q. 9. The monitoring, with notice, at a later time period by a superior of an employee's emails is ethical.

Q. 10. The secret collection of data from an employee's computer at a later time period for review by a superior is ethical.

Q. 11. It is ethical for a superior to secretly listen-in on an employee's business related telephone calls.

Q. 12. The monitoring, with notice, at a later time period by a superior of an employee's computer screen is ethical.

53 percent of the employees strongly disagreed to the secret simultaneous monitoring by a superior of their emails as ethical. But interestingly, around 47 percent were of the opinion, that they utilized most of their work day in corresponding with official emails, and had no problem whatsoever, if the superior checked them. They claimed that they hardly had time to check their personal emails, at office and did so at home in a relaxed manner without the fear of electronic eavesdropping.

90 percent of the employees strongly disagreed with the statement that it is ethical for a superior to listen-in, with notice, on an employee's business related telephone calls. The senior level employees had more problems with this issue, and the researchers observed during data collection that the entry level employees were alright with the same issue.

Around 63 percent of the employees strongly agreed to the statement that monitoring, with notice, at a later time period by a superior of an employee's emails is ethical. The other 37 percent disagreed to the same. Therefore, it is a mixed reaction between employees on the same issue.

53 percent of the employees strongly disagreed to the secret collection of data from their computer at a later time period for review by a superior as ethical. Around 46 percent of them thought it was alright for their superiors to secretly collect the data at a later time

period. They claimed that this gives them less negative feeling, as many a times they are even unaware of such an act by the superior.

46 percent of the employees strongly agreed that it is ethical for a superior to secretly listen-in on an employee's business related telephone calls. They claimed that most of their calls are official ones, and there is nothing that is confidential to be kept away from the superior, unless the employee is resorting to some unethical practice himself at the stake of the organization. Whereas 53 percent of the employees strongly disagreed to the same and considered this act as unethical.

The monitoring, with notice, at a later time period by a superior of an employee's computer screen was considered ethical by 43 percent of the employees, and around 46 percent of them strongly disagreed and deemed it to be unethical. Most of the employees upon discussion agreed that few employees resort to cyber slacking (surfing the internet for non-work related activities), and that effects the overall perception of employers to employees, and the resultant is such electronic monitoring.

Q. 13. It is ethical for a superior to secretly record an employee's business related telephone calls for later review.

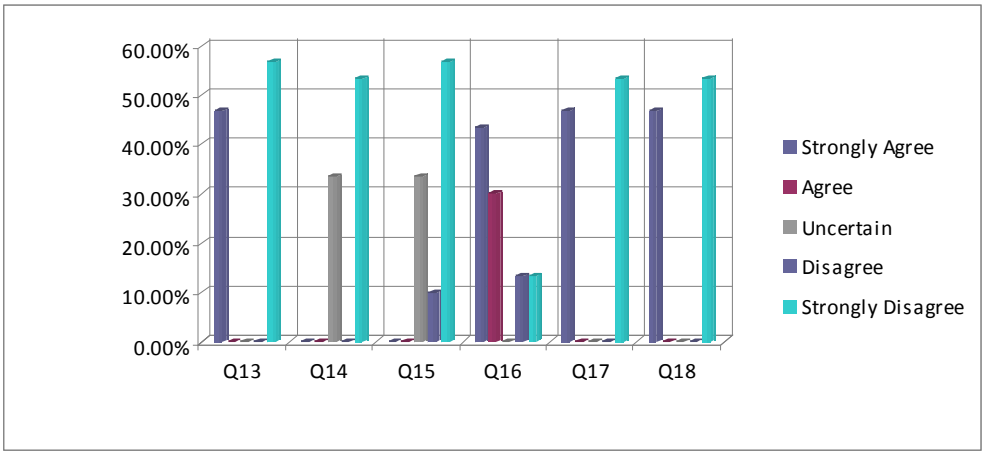
Q. 14. The secret simultaneous monitoring by a superior of an employee's computer screen is ethical.

Q. 15. The simultaneous monitoring, with notice, by a superior of an employee's emails is ethical.

Q. 16. It is ethical for a superior to record, with notice; an employee's business related telephone calls for later review.

Q. 17. The secret monitoring at a later time period by a superior of an employee's computer screen is ethical.

Q. 18. The secret monitoring at a later time period by a superior of an employee's emails is ethical.



Graph 3: Employee Opinion on their Superiors Electronic Monitoring Techniques.

57 percent of the employees strongly disagreed to their superiors secretly recording an employee's business related telephone calls for later review as an ethical act, and the other 43 percent did not have any apprehensions on the same issue. So, once again we can observe

the differences in the perception and opinion of employees towards their superior's electronic monitoring techniques. Perhaps the employees who strongly agreed to this as an ethical act, have adapted to the working lifestyle in Dubai, and know for sure that electronic monitoring has become a state-of-the art technique in today's workplace.

53 percent of the employees strongly disagreed to the secret simultaneous monitoring by a superior of an employee's computer screen as ethical. 33 percent claimed that they were uncertain as to whether such an act is ethical or unethical. The employees had one reservation that they discussed with the researchers, and that was, what is the guarantee that the superiors are doing the right thing by this secret monitoring, and could be even taking up a personal vengeance in the name of organization requirement of monitoring. The researchers do agree to this point to a large extent, as many a scores of superior-subordinate conflicts can be settled with such menial acts of intruding into the subordinates work privacy in totality.

The simultaneous monitoring, with notice, by a superior of an employee's emails is ethical statement was strongly disagreed by 67 percent, and 33 percent were again uncertain about the same. Therefore, it is clearly visible that employees do not like the technique of secret or with notice monitoring of their emails.

73 percent of the employees strongly agreed that it is ethical for a superior to record, with notice; an employee's business related telephone calls for later review. Around 26 percent of the employees only strongly disagreed on the same. Therefore, the researchers consider this a positive trend, as it is clear that the employees of all the three MNCs have reason in accepting the fact that electronic monitoring with notice of telephone calls is ethical, although that was not the same for email monitoring.

The secret monitoring at a later time period by a superior of an employee's computer screen/email is ethical as a statement was strongly disagreed by 53 percent of the employees and around 46 percent strongly agreed to the same. It can be clearly understood that the employees were not very comfortable and deemed it unethical with the electronic monitoring regarding emails and computer screens especially by their immediate superiors.

Therefore, from the analysis it is clear that from the ethical dimension perspective, employees were positive about occasional electronic monitoring of business related telephone calls, computer screens and emails. They considered it highly unethical for their superiors to monitor their computer screens and emails, instead preferred the IT department to do such acts, but definitely not on continuous basis. They clearly stated that secret monitoring eventually creates a lack of trust and commitment between the management, superiors and employees that their morale towards the organization decreases. So, the corporates need to pay heed to this factor too while planning out on the different techniques of electronic monitoring.

Suggestion and Conclusion

Organizations should create an "Acceptable Use Policy" (AUP) that covers e-mail, internet and applications, and that AUP should be clearly communicated to employees. Should an organization fail to create or communicate an AUP, it will be exposing itself to a myriad of legal problems. The AUP must be carefully drafted, and make absolutely clear what is and is not permissible. Do you want to impose a blanket ban on personal surfing? Or permit it only during coffee and lunch breaks? Do you want to prohibit the use of peer-to-peer applications? What type of content should employees be prohibited from accessing? To what extent should employees be permitted to send personal e-mail?

To be effective, an AUP must be underpinned with a monitoring mechanism. If it is not then, some employees will intentionally or unintentionally fail to adhere to the rules – and that is something which could prove to be extremely costly to the organizations resources as well as reputation.

Therefore the conclusive evidence from this study suggests that employees view E-monitoring as ethical as long as notice is provided to them that they are under surveillance. Companies wishing to operate within the United Arab Emirates business environment as part of the Middle East regional market should not have problems with the electronic monitoring of their employees as long as it is carried out in a professional and ethical manner with sufficient notice to the employees. This will enable in gaining the trust and commitment of the employees, and strengthen the organizational culture as well as employee morale.

References

Bylinsky, G. (1991), "How Companies Spy on Employees", *Fortune*, Nov. 14, pp.131-141.

Douglas, P.C. and Wier, B. (2005), "Cultural and Ethical Effects in Budgeting Systems: A Comparison of U.S. and Chinese Managers", *Journal of Business Ethics*, Vol. 60 (summer), pp.159-174.

Electronic Monitoring, *http://legal- dictionary.thefreedictionary.com.*

Flynn, Nancy (2005), "Electronic Monitoring & Surveillance Survey", *http://www.epolicyinstitute.com/survey2005Summary.pdf. Accessed 30 August, 2010.*

Flynn, Nancy (2007), ePolicy Handbook, ePolicy Institute, *http://www.epolicyinstitute.com/survey2007Summary.pdf. Accessed 30 August, 2010.*

Forsyth, D.R. (1980), "Taxonomy of Ethical Ideologies", *Journal of Personality and Social Psychology*, Vol. 39, No. 1, pp.175-184.

Goessl, L. (2010), "How employers monitor employees at work", *www.helium.com*, 2nd September 2010.

HSBC Bangalore suffers £233,000 security breach, *http://news.zdnet.co.uk.*

Kallman, E. (1993), "Electronic Monitoring of Employees: Issues and Guidelines", *Journal of Systems Management*, (June), pp.17-21.

Kelly, Eileen P. (2001), "Electronic Monitoring of Employees in the Workplace", National Forum, Vol. 81, No. 2, pp.4-6.

Kidwell, R.E. and Bennett, N. (1994), "Electronic Surveillance as Employee Control: A Procedural Justice Interpretation", *The Journal of High Technology Management Research*, Vol. 5, No. 1, pp.39-57.

Laabs, J.J. (1992), "Surveillance: Tool or Trap?" *Personnel Journal*, (June), pp.96-104.

Redfern, K. and Crawford, J. (2004), "An Empirical Investigation of the Ethics Position Questionnaire in the People's Republic of China", *Journal of Business Ethics*, Vol. 50, pp.199-210.

Roxas, M.L. and Stoneback, J.Y. (2004), "The Importance of Gender across Cultures in Ethical Decision-Making", *Journal of Business Ethics*, Vol. 50, pp.149-165.

Snell, R.S. and Herndon, N.C. Jr. (2004), "Hong Kong's Code of Ethics Initiative: Some Differences between Theory and Practice", *Journal of Business Ethics*, Vol. 51, pp.75-89.

Turner, R., "Employee Monitoring: An essential component of your risk management strategy", *www.effortz.com. Accessed 5 September, 2010.*

Vaught, B.C., Taylor, R.E., and Vaught, S.F. (2000), "The Attitudes of Managers Regarding the Electronic Monitoring of Employee Behavior: Procedural and Ethical Considerations", *American Business Review*, Vol. XVIII, No. 1 (January), pp.107-114.

Workplace Privacy and Employee Monitoring, Empowering Consumers, Protecting Privacy, *http://www.privacyrights.org/ar/Privacy-IssuesList.htm,* 2nd September, 2010.

Wu, Chen-Fong (2004), "Research on a Typology of Business Ethics Operation across the Taiwan Strait", *Journal of Business Ethics*, Vol. 52, pp.229-242.