Global Journal of Management and Business Research: A
Administration and Management
Volume 15 Issue 11 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 2249-4588 & Print ISSN: 0975-5853

Internet Access, use and Monitoring Policies in Selected Organisations in Ibadan, Nigeria

By Adeoye Adetola Atinuke & Adelowo Oluremi Titilope

National Open University, Nigeria

Abstract- The Internet has revolutionized, and continues to profoundly affect, the way one does business. Since the Internet has become a main source of communication both within and outside organizations, they are caught between providing Internet access to employees to perform job related activities and monitoring employees' use of Internet without infringing on their rights and privacy. This study therefore examined the extent of Internet access and use, pervasiveness of Internet monitoring, availability of Internet use policy and compliance to Internet use policy in the selected organisations.

The study adopted ex post facto survey design. Stratified random sampling was used to select 246 organisations comprising those in public, private, not for profit and non-governmental sectors. An adapted questionnaire from Alampay and Hechanova's 2008 study was used to collect data from the organisations. One hundred and eighty three (74.4%) copies of returned questionnaires were used for data analyses.

Keywords: *internet monitoring; employee monitoring; ibadan; internet use policy.*

GJMBR - A Classification : JEL Code: L29

Internet Access, use and Monitoring Policies in Selected Organisations in Ibadan, Nigeria

Adeoye Adetola Atinuke [α] & Adelowo Oluremi Titilope [σ]

Abstract- The Internet has revolutionized, and continues to profoundly affect, the way one does business. Since the Internet has become a main source of communication both within and outside organizations, they are caught between providing Internet access to employees to perform job related activities and monitoring employees' use of Internet without infringing on their rights and privacy. This study therefore examined the extent of Internet access and use, pervasiveness of Internet monitoring, availability of Internet use policy and compliance to Internet use policy in the selected organisations.

The study adopted ex post facto survey design. Stratified random sampling was used to select 246 organisations comprising those in public, private, not for profit and non-governmental sectors. An adapted questionnaire from Alampay and Hechanova's 2008 study was used to collect data from the organisations. One hundred and eighty three (74.4%) copies of returned questionnaires were used for data analyses. Descriptive statistics specifically frequency, percentage distribution and cross tabulation were used for data analyses.

Findings revealed that two-third of the organisations provide Internet access to employees depending on their job category. However, some organisations monitor employee Internet use and also have Internet use policy. Majority of the organisations are concerned about the content accessed by their employees and therefore blocked some online content and applications particularly those related to pornography, gaming and social networking. Most organisations reported difficulties with employees' excessive chatting that is non-work related and accessing pornography at work. In addition, private organisations monitor employees' Internet use most.

The results suggest the need for more organizations to articulate their policies on Internet use, educate workers on Internet security and formulate mechanisms to ensure the integrity of employee monitoring. Thus, organisations need to invest on the formulation of Internet use policy that will protect both the organisations and employees.

Keywords: internet monitoring; employee monitoring; ibadan; internet use policy.

I. Introduction

The Internet has revolutionized, and continues to profoundly affect, the way one does business. It is now a critical (if not the main) tool and venue for conducting commerce. As a tool, it allows buyers and sellers nearly unlimited access to information, goods and services. As a venue, it does away with the limits of geography, the time zones and, in some cases, the need for a physical office. With its tremendous potential, it has become commonplace for businesses and consumers to utilize the Internet for a variety of transactions ranging from emails to actual online purchases (United Nations, 2007). The Internet has a range of capabilities that organizations are using to exchange information internally or to communicate externally with other organizations. The primary infrastructure for e-commerce, e-banking, e-business, e-learning and virtual library is provided by the Internet technology (Ureigho et al, 2006).

The Internet as a global village is a compendium of information, a library of fun, a shopping mall, health institute of a kind, a research institute, an archive, a musical studio and a pornographic shop amongst other things. The word Internet is derived from two words: "international" and "network". The Internet therefore can be defined as an international computer network of information available to the public through modem links (Bassey, 2003). It is an international network of networks that is a collection of hundreds of thousands of private and public networks all over the world. There are rich and varied learning experiences available on the Internet that would have been inconceivable just a short while ago (Anonymous, 2001). The vast information on the Internet that covers almost all areas of human endeavours has made the Internet the greatest achievement of the Century. The Internet is fast becoming a necessity for every economy (Alese and Owoyemi, 2004).

Since the Internet has become a main source of communication both within and outside organizations, companies ask their employees to use the Internet extensively for communication as well as for business activities. The Internet is cost-effective and is faster than other communication media, making it easy for employers to coordinate their global activities of customers and suppliers (Lehr and Lichtenberg, 2000). Realizing this, the Internet has found a place as a backbone of communication infrastructure in many organizations and has made possible the flattening of corporate structure for communication and dissemination of information. This has certainly benefited companies by increasing productivity and creating avenues to explore new market opportunities (Anonymous, 2001). Today, many companies let their employees work from home because it is more

Author α: e-mail: adetola.adeoye@gmail.com
Author σ: National Open University of Nigeria.
e-mail: Stremy62@gmail.com

economical and more productive. For many global business firms, reduction in the cost of disseminating information and improvement in the speed of qualitative decision-making has been possible only due to use of the Internet. Many observations agreed that the Internet has not only boosted the productivity in the organizations but has also created a sense of empowerment among workers (Stratopoulos and Dehning, 2000).

There is no denying that the use of Internet in organizations has made employees more efficient and has improved communication channels. Undoubtedly it also affected organizations' employees and their workplaces in job design, conditions of work and other (numerous) ways. As noted by Barley 1996:

> *"Future prosperity is likely to hinge on the use of scientific and technical knowledge, the management of information and the provision of services. The future will depend more on brains than brawn"*

However, the Internet has also opened up new areas of concern such as its effect on workers' productivity (Anonymous, 2001). Stories of workers who abuse the Internet for their self-gain or at times malign the image of the organization are finding a place in the headlines of many news journals. Employees spend time surfing the net, communicating with their friends, relatives and counterparts during working hours, (Ferris, 2000) checking their stock prices, shopping for travel bargains and exchanging personal e-mail via the Internet while at work - even though their companies prohibit these activities (Marsan, 2000).

According to IBM Global Business Security Index (IBM, 2004), 28,327 new viruses were discovered in 2004 and this increased the number of known viruses to 112,438. Traditionally, viruses and other malicious software (malware) are hidden in e-mail attachments and malicious codes are also embedded in joint photographic experts group (jpeg) and bitmap pictures, so when employees visit websites with hacked or intentionally prepared images, their computer system get infected and thus affects their productivity(Telenor, 2004). Employees' misuse of the Internet can be an avenue for virus attacks on organisations system which will slow down performance and might eventually destroy the affected system. Although there are several means of detecting, containing and deleting malware, they still cannot protect the computer systems before they are exposed to the threat (Deisz, 2005).

The purpose of this study is to investigate the extent to which organisations in Ibadan monitor their employees Internet use and how Internet facilities are regulated. It also aims to know if there are organizational ICT policies in place to guide Internet use and whether such policies are made known to the employees. This study will assess the extent of problem that is encountered in the misuse of the Internet by the employees in the organizations and the disciplinary actions being imposed. It is intended to look at practices and attitudes among organisations in Ibadan regarding access to the Internet and monitoring of its use in the workplace.

What do employees use the Internet for in the organisations? Reports indicate that about 55 million people in the United States access the World Wide Web ("the Web") from their workplace on a daily basis (Horrigan, 2002). A Department of Commerce study indicates that Web usage in the workplace has a growth rate of approximately 54% per year (U.S. Department of Commerce, 2002). While such growth has the potential to increase worker productivity, it is not without significant problems (Lim et al., 2002; Simmers, 2002). The American Management Association indicates that more than 50% of all workplace-related Web activities are personal in nature (Greengard, 2000). Another study indicates that, on average, employees spend 8.3 hours a week surfing the Web for non-work-related activities (Websense, 2002). These activities include online entertainment, reading news, making travel arrangements, online purchases, and searching for jobs. Such activities translate into billions of dollars a year in revenue lost due to lost productivity (Mills et al., 2001). More so, personal web usage has caused organizations to face a host of other detrimental issues (Siau & Nah, 2002). There is an increased burden on company servers as bandwidth and system storage gets clogged with non-work-related files (Mills et al., 2001). Organizations also face heightened security risks from viruses and other malicious programs inadvertently downloaded by employees as they use the web for personal reasons (Sloane, 2002).

In another survey conducted in 2006 by Telemate.Net Software, Inc., a provider of Internet usage management and e-Business intelligence solutions, the survey covered 700 companies from a diverse cross-section of industries in America. Survey respondents included executives, senior Information Technology (IT) professionals, IT and human resource managers. Findings indicated that 83% of companies were concerned with inappropriate employee usage of the Internet and the resulting legal liabilities and/or negative publicity. Over 70% indicated that employee Internet abuse results in real costs to their companies in the way of additional network upgrades, lost productivity and slow network response. The concern about Internet abuse and the associated legal liabilities, negative publicity and excessive costs was consistent across industries, company size and job titles of the respondents (Business Wire, 2000).

In a survey of public companies carried out in South Africa (Dancaster, 2001), findings reveal that: 69% experience loafing on the Internet; 70% experience accessing, downloading or sending through e-mail of discriminatory or sexually offensive jokes or pictures;

65% experience clogged bandwidth or degraded system performance through abuse of the Internet system; 6% experience the violation of copyright laws or the posting of information in the name of the company that defames other companies or individuals; 60% have disciplined employees for Internet and email abuse; and 77% have reserved the right to monitor online traffic at any time. These results imply that there is a need to monitor employees' use of the Internet so as to prevent the organisations and reduce loss in productivity.

While most of the studies have been carried out in the highly developed countries (United States and United Kingdom), only the South African survey by Dancaster represents an emerging or developing countries' situation on monitoring employees Internet use. Several studies have been carried out on the use of Internet in many professional areas in Nigeria like; banking, health, insurance, education, legal practices and lots of more, these surveys have emphasised that the Internet is improving and increasing productivity(Adebayo, 2006; Awoleye, et al, 2008; Omolase, et al, 2010; Longe and Chimeke, 2008; Madueme, 2010; Olatokun and Adeboyejo, 2008). Although all these studies have shed some light on the impact and benefits of the Internet, none of them focused on the misuse of Internet in the workplace which is why this study seeks to know how employees use the Internet provided by their organisations and how such use is monitored. Also, this study will be a guide to future researches in this area of Internet use in organisations.

a) *Internet Use in the Nigeria workplace*

Nigeria, although a Less Developed Country (LDC), is one of the largest economies in the Sub-Sahara region of Africa (Feldman, 1992) and many major multinational corporations and their affiliates conduct business there (Jason, 1997; Thompson, 1994). In Nigeria the Gross Domestic Product (GDP): purchasing power parity is $110.5 billion (1999 est.), the per capita purchasing power parity is $970 (1999 est.) and in 1999 the number of Internet Service Providers (ISPs) is 5 (CIA 2000 World Factbook).

The Internet usage trend is Nigeria has changed in a short period of time, In December 2000, Nigeria had 450,000 connected fixed lines, no connected digital mobile line, 1 national career, 18 operating Internet Service Providers, 9 active licensed fixed-line operators, and 1 licensed mobile line operator (Ndukwe, 2005). In the same period, Nigeria had 200,000 Internet users (Internet World Statistics, 2005), even though many experts disagree with the figures. In March 2004, the figures grew to become 888,854 connected fixed lines, 3.8 million connected digital mobile lines, 2 national careers, 35 operating Internet Service Providers, 30 active licensed fixed-line operators, and 4 licensed mobile line operators. In December 2004, Nigeria had 1.5 million Internet users, a penetration rate of 1.3% and constituted about 5.6% of the total number of African Internet users. Africa itself only boasts of 1.5% of global Internet users even though it has 14% of the world's inhabitants. Summarily, Nigeria's ICT space has improved significantly from 400,000 lines in 1996 to over 71.9 million lines in October 2009(Nigerian Communications Commission figures 2010), and 43,985,000 Internet users in 2010(World Internet Users). In Nigeria, researchers have not really studied the organizational use of the Internet and so there is little to show about how employees use the Internet and even their computers.

According to a study carried out by Simmers and Anandarajan (2004) on Web Usage in the workplace in Nigeria, Malaysia and the United States, a total of 237 questionnaires were administered in 19 organisations(Manufacturing=4%, Services=41%, Wholesale, retail trade=5%, Finance, Insurance, Real Estate=30%, Education=2%, Government=4%, Self-employed=0% and Other=14%) in Nigeria. The study revealed that 224 (94.5%) employees have access to the Internet in their organisations, 28.3% block access to certain web pages, 60.1% has clearly stated policies on Internet usage, 59.6% has additional passwords for web access and 29.0% strictly enforces its Internet policies. Furthermore, the study revealed that Nigerians most likely access business and financial pages (mean=3.79), sports and news(mean=3.73), general interest (mean=3.84), arts and entertainment (mean=3.08), travels and leisure(mean=2.96) and competitor's webpage(mean=3.24) from workplaces. Also the study shows the employees attitude towards personal web searching at work (mean=3.77) which interpret that most of the employees enjoy personal web usage during work hours or at workplaces.

Internet usage is still in its infancy in Nigeria. Many authors have written about Internet connectivity in Nigeria. According to Adeya and Oyeyinka (2002) the level of access and connectivity is far below that of developed countries. Nigeria as a whole has only two percent of the Internet connectivity in the developed world. This is improving as a result of many universities and other institutions achieving direct access either through telecommunication or VSAT (wireless). As access grows, Nigerian researchers, scholars, and the general public have the opportunity to undertake research, teaching, learning, and other activities via the Internet.

b) *Previous Studies on Monitoring Internet use in workplace*

A 2007 survey by the American Management Association and the e-Policy Institute found that two-thirds of employers monitor their employees' web site visits in order to prevent inappropriate surfing. And 65% use software to block connections to web sites deemed off limits for employees. This is a 27% 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, an external blogs. Of the 43% of companies that monitor e-mail, nearly three-fourths use technology to automatically monitor e-mail. And 28% 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% monitor blogs to see what is being written about the company. Another 10% monitor social networking sites.

In a similar survey carried out in Malaysia by Yulihasri et al in 2006 on use of Internet in Malaysian workplace, the employees agreed that it is acceptable to use Internet for personal searches(mean= 3.82), surf Internet while at work(mean= 3.82) and even access sexually explicit websites if they are alone in their offices(mean= 3.77). It was also noted that Internet usage policies and careful usage did not get high level of agreement because their standard deviation are large (1.013 and 0.926) which shows that the employees are ignorant about acceptable use policies in the organizations or they just do not care.

According to a survey by Alampay and Hechanova (2010) on monitoring Internet use in workplaces in Philippines, a total of 112 organizations was surveyed and it reveals that 65% of the organizations surveyed gave Internet access to all its employees which show that the Internet have become more integrated into organizations and people's work. Even though access is provided, 58% block some sites and that larger organization restricts Internet access. Most organizations (57%) monitor and review their Internet connections while 38% do not. The study also reveals that a little than half of the organizations surveyed have clear written organizational policies on Internet use, email use and use of instant messaging and what appears to be lagging is the articulation and implementation of Internet use policies which is the reason why Philippines organizations are encountering negative consequences including security breaches and diminished productivity. Though in some cases misuse of Internet has lead to discipline and even dismissals.

In the survey by Simmers and Anandarajan (2004) on Web Usage in the workplace in Nigeria, Malaysia and the United States, a total of 237 questionnaires were administered in 19 organisations(Manufacturing=4%, Services=41%, Wholesale, retail trade=5%, Finance, Insurance, Real Estate=30%, Education=2%, Government=4%, Self-employed=0% and Other=14%) in Nigeria. The study revealed that 224 (94.5%) employees have access to the Internet in their organisations. Also reveals that 28.3% of the companies blocked certain web pages, 59.6% uses additional passwords for web access, 60.1% have clearly stated Internet use policies and only 29% strictly enforces its Internet policy.

II. Methodology

a) *Policy Compliance and Discipline*

Table 4.1 presents the results of the analysis of the pattern of policy compliance and disscipline across the organisations. the results shows the organisations that have complined and disciplend an employee on Internet misuse.

Table 4.1 : Policy Compliance and Discipline

Variables	Yes(%)	No(%)
Has your organization ever disciplined an employee on misuse of office Internet facilities?	31.1	68.9
Has your organization ever disciplined for misuses of company email?	28.4	71.6

From table 4.1 the result shows that 31.1% of the organizations have ever disciplined an employee on misuse of office Internet facilities and 68.9% has not disciplined any employee. It also shows that 28.4% have ever disciplined an employee for misuse of company email and 71.6% has not disciplined an employee on misuse.

Table 4.2 presents the result of the analysis of the forms of disciplinary actions that the organizations have taken against the employee that misuse the Internet facilities.

Table 4.2 : Type of discipline

Variables	Dismissal (%)	Formal Warning (%)	Informal Warning (%)	Other form of discipline (%)	No response (%)
What form of discipline was taken on misuse of office Internet facilities	1.6	25.1	2.7	1.6	68.9
What form of discipline was taken on misuse of company email	1.6	25.1	1.6	0	71.6

From table 4.2 the result shows that only 1.6% of the organizations that was surveyed have dismissed employee on misuse of office Internet facilities and company email. It also revealed that 25.1% have formally warned their employees on misuse of office Internet facilities and company email. While 2.7% and 1.6% have informally warned their employee on misuse of office Internet facilities and company email respectively. And 1.6% has used other forms of discipline.

III. Test for Association Between Variables using Cross Tabulation

a) *Internet Access and use*

Table 4.3 and presents the result of the cross tabulation analysis between organisation type and who has access to Internet in the organisations.

Table 4.3 : Access by type of organization

Type of organization	Who has access to Internet in the organization						Total	
	All		Only management		Depending on job			
	Frequency	%	Frequency	%	Frequency	%		
Government	8	4.4	5	2.7	17	9.3	30	16.4
Private	22	12.1	25	13.7	82	44.8	129	70.5
For profit	2	1.1	1	0.5	12	6.6	15	8.2
NGO	5	2.7	1	0.5	3	1.6	9	4.8
Total	37	20.3	32	17.4	114	62.3	183	100

Chi Square Test

	Value	Df	Asymp. Sig. (2-sided)
Pearson Chi-Square	10.808[a]	6	.094

From table 4.3 the results shows that 20.3% provide Internet access to all employees out of which the private organisations have the largest percentage of 12.1%. It also shows that 17.4% provide Internet access to only management staff with the private organisations with the highest percentage of 13.7%. Furthermore, the table shows that 62.3% provide Internet access to employee depending on their job description with 44.8% from the private organisations. The Pearson chi-square value is 0.094 which shows that there is no significant association between type of organization and who has access to Internet in the organisation.

Tables 4.4 and presents the results of the cross tabulation analysis between who has Internet access and Industry type. This table will show the association between the type of industry and who has Internet access across the organisations.

From table 4.4 the result shows that there is an association between who has access to Internet in the organisations and industry type with the Pearson chi-square value of 0.000. Majority provided access to employees depending on their job(n= 114) description, the more discriminating, in terms of providing access, were public administration/ government(n=7) organisations.

Table 4.4 : Access by Industry type

Industry type	All		Only mgt/supervisor		Depending on job		Total	
	Freq	%	Freq	%	Freq	%	Freq	%
Business/professional service	9	4.9	3	1.6	15	8.1	27	14.6
Research	5	2.7	1	0.5	8	4.4	14	7.6
Wholesale/Retail	2	1.1	3	1.6	1	0.5	6	3.2
Public admin/govt	2	1.1	2	1.1	3	1.6	7	3.8
Financial Services	4	2.3	3	1.6	55	30.1	62	34.0
Manufacturing	1	0.5	7	3.9	9	4.9	17	9.4
Infor/Comm/Media	8	4.4	2	1.1	7	3.9	17	9.4
Education/ School	1	0.5	2	1.1	7	3.9	10	5.5
Others	5	2.7	9	4.9	9	4.9	23	12.5

Industry type	All		Only mgt/supervisor		Depending on job		Total	
	Freq	%	Freq	%	Freq	%	Freq	%
Business/professional service	9	4.9	3	1.6	15	8.1	27	14.6
Research	5	2.7	1	0.5	8	4.4	14	7.6
Wholesale/Retail	2	1.1	3	1.6	1	0.5	6	3.2
Public admin/govt	2	1.1	2	1.1	3	1.6	7	3.8
Financial Services	4	2.3	3	1.6	55	30.1	62	34.0
Manufacturing	1	0.5	7	3.9	9	4.9	17	9.4
Infor/Comm/Media	8	4.4	2	1.1	7	3.9	17	9.4
Education/ School	1	0.5	2	1.1	7	3.9	10	5.5
Others	5	2.7	9	4.9	9	4.9	23	12.5
Total	37	20.3	32	17.4	114	62.3	183	100

Chi Square Test

	Value	Df	Asymp. Sig. (2-sided)
Pearson Chi-Square	55.262[a]	16	.000

Results showed that the more information intensive organisations (Information, Communication and Media) tend to provide access to everyone. Financial services industry (n=55) provides Internet access to employees depending on their job because their business depend on the Internet for successful and quick transactions.

Table 4.5 presents the result of the cross tabulation analysis between industry type and nature of Internet restrictions across the organisations. This is to test the association between the two variables.

Table 4.5 shows that there is a significant association between industry type and some applications are blocked because the Pearson Chi-square value is 0.000, it also shows that 55.7% of the organizations blocked some application with the financial services having the highest (32.2%, n= 59). It also reveals that there is association between industry type and all form of restrictions except other types of restrictions (chi-square sig value=0.263) described by the respondents.

Table 4.5 : Industry type and blocked applications

INDUSTRY	Application blocked		Blocked can be accessed after work		Some computers have access		Accessible on job		Accessed with permission		Other types of restriction	
	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%
Business/professional service	4	2.2	3	1.6	4	2.2	1	0.5	5	2.7	0	0
Research	6	3.3	3	1.6	2	1.1	0	0	6	3.3	1	0.55
Wholesale/Retail	1	0.5	0	0	2	1.1	1	0.5	0	0	0	0
Public admin/govt	6	3.3	1	0.5	5	2.7	0	0	2	1.1	0	0
Financial Services	59	32.2	51	27.9	8	4.4	1	0.5	4	2.2	0	0
Manufacturing	9	4.9	3	1.6	5	2.7	4	2.2	4	2.2	0	0
Infor/Comm/Media	6	3.3	3	1.6	9	4.9	3	1.6	4	2.2	1	0.55
Education/ School	4	2.2	0	0	5	2.7	2	1.1	1	0.5	0	0
Others	7	3.8	2	1.1	5	2.7	0	0	1	0.5	0	0
Total	102	55.7	66	36.1	55	30.1	12	6.6	27	14.8	2	1.1

chi-square test

Pearson Chi-Square	Application blocked	Blocked can be accessed after work	Some computers have access	Accessible on job	Accessed with permission	Other types of restriction
Value	74.497[a]	88.906[a]	29.053[a]	21.273[a]	18.836[a]	10.028[a]
df	8	8	8	8	8	8
Asymp. Sig. (2-sided)	.000	0.000	0.000	0.006	0.016	0.263

b) *Internet Monitoring and Usage*

The test for association was between one of the demographic variables which is the type of industry and questions “who monitors Internet connection in the organization?”, “what do you monitor?”, “which of the following are restricted?” and “has your organization experienced any problem with regard to employee Internet use?” Table 4.6(see appendix) presents the result of the cross tabulation analysis between industry type and what is monitored in the organisation.

From table 4.6, the result shows that 60.1% monitor content accessed on the Internet by their employees with the highest of 32.2% from the financial services industry and the least of 0% from the wholesale and retail industry. It also shows that only 1.6% monitor personal blogs of employee. Table 4.6 shows that content accessed on the Internet by employees have a significance association with industry type with a Pearson chi-square value of 0.000 which is significance. Table 4.7(see appendix) presents the result of the cross tabulation analysis between industry type and what is restricted on the organisations Internet facilities and the Pearson chi-square test between the two variables.

Results showed that 74.7% of the organisations surveyed block pornography sites, 59% blocked online gaming sites, 46.4% block social networking sites, 55.2% blocked downloading sites, 38.8% blocked yahoo messenger, 37.2% blocked Skype, 33.9% blocked online mail services sites, 36.1% blocked blog sites and 11.5% agreed to blocking other sites like competititor’s sites, entertainment sites, online shopping sites, and many more. It also reveals that the financial services industry blocked almost all the sites except for News site that has the least percentage of 2.2% which is also the same with other industries. The Pearson chi-square value also shows that there is an association between the industry type and all sites except News sites which has the significance value of 0.740 which is above the threshold value of 0.05. Thus it shows that there is no association between the type of industry and the news sites.

IV. Discussion of Findings

a) *Organisations Profile*

The results of the study shows that private organisation with small employee size are the most users of the Internet for their business transactions, just a few of the government owned organisation have Internet access. It also reveals that the majority were private organisations with the predominant type of industry is the financial services. This is so because these industries rely on the Internet as the backbone for successful business transactions nationwide. This findings differs from a similar study carried out in the Philippines by Hechanova and Alampay (2010) that reported that the predominant organisation type that have Internet access was retail and trade and that the large size organisations were the most users of Internet.

b) *Internet Access and Use*

The results of the study shows that the organizations surveyed have Internet access and mostly make use of the Local Area Network and Wireless Fidelity connections which shows that providing access to the Internet is becoming the norm among organisations in Ibadan. Moreso, over half of the organisations provide access to employees depending on their job description; and a few said it is available to all employees which deviates from what Alampay and Hechanova(2010) described in a similar study in the Philippines that the higher percentage of access was granted to all employees. It also shows that more than half of the organisations that have Internet access restrict their employees’ access to the Internet and only few give employees complete access. This finding also agrees with the survey of 670 companies by carrier site Vault.com which examined Internet monitoring, the results indicate that 41% of organizations restrict or monitor Internet use (Net Monitoring Survey, 2000). The reason that could be adduced for providing access to Internet was for easy communication between offices (financial services and information, communication and media) and aids research findings (research institutes, education/school and information, communication and media). Respondents also perceived that access to the Internet would lead to higher productivity among employees. This agrees with the findings of Alampay and Hechanova(2010) that the popular reason for providing Internet access to employees was for research and making communication easier.

c) *Internet Monitoring and usage*

Although Internet access is provided, a little below half of the organisations monitor websites connections of all employees and for selected job categories while a larger percentage does not restrict usage of the Internet. Also, a little below half of the organisations have written policy on Internet use and some uses a dedicated MIS staff and automated software to monitor Internet. In addition, majority of organisations that block some applications also agreed to the fact that some of the blocked sites can be accessed after work hours are private organisations and mostly the financial services industry.

However a few of the organisations reported that some applications can be accessed if permission is requested to justify why the websites are to be accessed. These restrictions are necessary so as to aid employees' concentration at work and would reduce traffic congestion on organisations servers. This finding agrees with the AMA survey of 2005 which showed that employers are increasingly concerned about inappropriate Web surfing, and 65 percent of employers use software to block connections to some web sites, a 27 percent increase over an earlier 2001 survey (AMA, 2005). But according to Alge (2001), employers should allow employees personal Internet time; exercising excessive control impedes ideas and innovation. The Internet is a productivity tool in that it makes communication quicker and more efficient. As a learning tool, it gives employees access to new knowledge, which makes them better in their jobs. Employees become both more effective and efficient. This increases their self-esteem, which improves customer service and interpersonal relationships (Singh, 2004). Therefore, it is not only discriminatory to allow only some employee's access to the Internet, but it is also being selfish. The results also revealed that the smaller organizations really monitor their employees' Internet use. This might be due to the fact that most of them are privately owned and are extensions of other offices with several branches and outlets across the country and it is the management's decision to put all office Internet use in the right order.

What organizations block and how they do so also varies. A lot of the organisations are bothered about the content accessed by employees through the Internet, although some of them check time spent and just a few monitor employees' personal blogs. Blocking of pornography sites is common but it has not however dissuaded people from trying to access such content as evident from the results of the study. Almost all the organisations block pornography and online gaming sites as this two sites can reduce employees' productivity level and also lead to lack of concentration and time wastage which is precious to the organisation. This agrees to the findings with the study of Deisz (2005) on Norwegian organisations that reported that 73 % of Norway active adult users accessed the Web at least once from work, 41% access the Web a majority of the time at work, and 15% go online exclusively at work. Some organisations block some social networking sites like facebook, twitter and the likes, as they also distract employees' from the job. Some organizations agreed that they block employees from downloading music, pictures and video as these sites clogs up the bandwidth and makes the Internet connection slow and also to protect their computer systems from viruses attached to the downloaded materials. Online mail services were blocked by most of the financial services industry as most communication is meant to be within the organisations and other branches across the nation and every employee has company email for communication and business transactions. Whitepapers (web@work, 2004), (Davies, 2001) and (SecuComp, 2005) all concluded that cyber-slacking (surfing the web at work) is a major problem in most companies and that 37% of American workers surf the Internet constantly at the job, and that more than a half of them often use the Internet for private purposes at work. Also Dancaster (2001) reported that 64 percent of employees use the Internet at work for personal interests; and 37 percent say they "surf the Web constantly" while on the job. Caroll(2007) also reported that 60 percent of online purchases occur during normal work hours, as does 70 percent of porn traffic. Social networking sites are also becoming a particularly tenacious distraction. But almost all the organisations do not block news sites this might be due to the fact that everybody needs to know what is happening around them and in the world generally.

Some communication applications' sites like Yahoo messenger and Skype were blocked by a little less than half of the organisations that were surveyed. Instant messaging was seen as a more problematic application especially in the financial services industry, as fewer organizations restricted the use of yahoo messenger, Skype and blogs. Some IT managers indicated that their organisations allowed internally developed instant messaging devices that could allow their employees communicate with themselves. This further illustrates the recognized importance of these applications, while also highlighting the security risks involved with using similar online-based services. As Villeneuve (2008) has claimed, trusting online services with personal communications may sometimes be misplaced. Majority of the organisations said employees' excessive chatting that is non-work related is a big problem they faced. Accessing pornography sites was not an uncommon problem too and likewise downloading of music, video and pictures, computer virus due to heavy downloads and playing online games as almost half of the respondents experience this problems. Alampay and Hechonava (2010) reported the same findings in their study.

d) Email Use and Computer Surveillance

Most of the organisations do not review or store employees email messages. Only a few agreed to do this for all employees and for selected job categories while a little above half do not. The organisations that do review company issued emails mostly do it routinely and only few do occasionally or when specified. It further shows that a little above half of the organisations review all employees' computer files, a few review for selected job categories and less than half do not review their employees' computer files. More so, few of those that store and review employees' computer files do it routinely and regularly. This finding disagrees with the American Management Association (AMA) study in 2005 that said that 3.63% employer's store and review employees' computer files. This implies that although some organisations store and review employees' computer files yet not all of them informed their employees' on organisations policy of monitoring files. The results also show that the private owned organisations were in the majority of those that store and review employees' computer files. In fact, the results also revealed that just a few of the organisations are bothered about what employees use their computer systems and emails for. This might be because most of them do not have enough resources in form of revenue and human capital for putting this process in place. It can also be due to the fact that most of the organizations' management staff does not have fore knowledge of the side effect of computer and Internet abuse.

e) Policy on personal use of ICTs

Findings shows that the development of clear and written organizational policies for using ICT facilities is in place in a little less than half of the organisations. Only few reported having email use and Internet use policies. Many private organisations, specifically financial services and information, communication and media already have policies in place and their policies are in compliance to industry regulations, although some are imposed by their head offices. Some of the information, communication and media services organisations are government owned and non-governmental organisations are the least advanced in developing policies for ICT-use. A few agreed on informing employees of organisation's policy on monitoring email messages and more than half did not inform their employees of the policy. This shows that just a few of the organisations actually informed their employees that there are policies governing the use of Internet. These findings agree in part with a similar study by Young and Case (2004) in America, the results indicate that 48% of the organizations had instituted an Internet Use Policy and 52% did not. Internet use policy is not fully utilized in the organisations and this may be because there are no policy developers or the management is ignorant of the use of policy for restricting and monitoring employee Internet use and the management is scared of breaching employees' privacy. Most employees believe they are entitled to a little of privacy when at work and they should be able to do anything in their private place but there should be balance between privacy and productivity. As noted by Signh 2004:

> *"An Internet policy is no different from any other organizational policy. Internet policies or Internet usage policies are designed to regulate the day-to-day usage of Internet facilities. Internet policies are designed to protect the rights of the employer and the employees, with regard to the use of Internet facilities. In many instances, policies are developed to ensure fairness and equity in the employer–employee relationship*."

The organisations that put policies in place said this act has helped to increase productivity but some argued that their employees would not be free at work and thus it may reduce their self-esteem and morale.

f) Policy Compliance and Discipline

A little above half of the organisations agreed to ever disciplining their employees on breaching company policy on ICT use. About half of those that agreed to ever disciplining their employees on breaching these policies were on misuse of office Internet and misuse of company email. Majority were issued formal warnings and few led to dismissals. The incidence of discipline is higher in small organisations than in the medium and large organisations showing that most of the organisations that reported having Internet use policy are implementing them and their employees are aware of the dangers of not complying. However, only few organisations with Internet or email use policy shows that many organisations are not aware of the importance of policies and have not experienced any legal issues on Internet misuse by their employees. This finding contrasts a finding of the American Management Association (AMA) in 2005, which reported that approximately 38% of 2,100 major U .S companies check their employee's e-mail and 54% monitor Internet connections (Yulihasri, et al, 2006). Of these organizations, 17% have fired employees, 26% have issued formal reprimands, and 20% have given informal warnings. The predominant industry that have complied and disciplined employees for inappropriate Internet and email use were the financial services and the information/communication/media industry, this is because they are branches to larger organisations. This may be due to the fact that the larger organizations are more likely to already have clear guidelines and policies, and may also have the dedicated resources in place for monitoring their information and communication systems.

V. Summary

The study investigated how employees' use of Internet is monitored in organisations in Ibadan, Oyo state, Nigeria. The study focused on Internet access and use, Internet usage and monitoring, employee email use, computer surveillance, policy on personal use of ICTs in the organisations and implementation of policies. It also examined how Internet is restricted and common Internet misuse problems. Relevant literature was reviewed on employee monitoring, Internet misuse in workplace and electronic monitoring. The literature reviewed also includes policy making and Internet use, computer monitoring and privacy issues. Similar research literatures on this study were also reviewed. The survey design approach was adopted. A structured questionnaire was used to collect data from 246 organisations in Ibadan out of which 183 were used for the analysis. Descriptive statistics was used to analyze the data using frequencies, pie chart and cross tabulation to test the association between the variables.

Findings showed that the small size organisations tend to use Internet for their day to day businesses. Also the private organisations provide Internet access than those in the government sector, for-profit and non-government organisations and the financial services industry dominates among the private organisations. Most government organisations in Ibadan do not provide Internet access to their employees. Furthermore, findings also revealed that most of the organisations make use of the Local area Network and Wireless fidelity to set up their Internet connections. It also showed that most organisation grant Internet access to employees based on job description (selected employees) with some restrictions. Some sites are blocked and some can be accessed with permission while some after working hours.

Findings equally showed that just a few of both the private and government organisations have Internet use policy and also informed their employees about the policy. Majority of employers are concerned about what is accessed by their employees and most of them use a dedicated MIS staff and automated software for the monitoring exercise; and the monitoring is mostly done routinely. It also showed that almost all the organisations block pornography sites and few blocked news sites; and excessive chatting that is non-work related and accessing pornography is the most problematic experience on Internet misuse by employees.

This study established that a little above half of the private and government organisations monitor employees' computer files, Internet and email messages routinely and also informed their employees about the policy governing such monitoring. Also, most of these private organisations that monitor employees' files and email messages are the financial services industry and they do so because of the integrity and nature of their business and most of the organisations that have Internet access do not have policy on Internet use.

The study revealed that the small organizations which are mostly private organizations had disciplined their employee on misuse of office Internet and company email. It further revealed that just one organization has dismissed an employee on misuse of the company's email and Internet, thus implementation of policy and compliance to policy is yet to find the right foot in the organizations.

VI. Recommendations

The study established that there is a need to put in greater effort to policy documentation and dissemination, employee education on Internet use and in establishing systems that will maximize the benefits of Internet technology while minimizing its risks.

More so, the organisations must balance employee productivity with privacy. If it is an organization's policy to store, review and monitor employee Internet use then such information should be protected. It also requires developing organizational capabilities to secure such information from outside intrusion and pressure. The researcher recommends that organisations should sensitize their employees on the content of Internet use policy so that they can be aware of the consequences if breached. Also, organisations should employ a good policy developer that would consider the employees privacy with respect to productivity so that the restrictions and guidelines will not affect employer-employee relationship, employee efficiency and organisation's productivity.

The limitations of this study are primarily a function of sample size and inadequate time. Even though responses were relatively equally distributed among organization size and industry type, a larger sample size would increase the robustness of results. Ultimately, results will assist organizations in improving employee Internet management, limiting risk, and maximizing employee productivity.

VII. Conclusion

Based on the findings of the this study, it can be concluded that most of the organisation surveyed in Ibadan have Internet access, use Local area network connection and are mostly private organisations. It also revealed that most employers grant Internet access to employees depending on their job descriptions and restricts their connections by using blocking software and a dedicated MIS staff. Content accessed on the Internet by employees is the major concern of the employers has pornography sites, online gaming sites and social networking sites were blocked by most of the organisations. In addition, most organisations that review and store employees email messages and computer files do it routinely. It can be concluded that most organisation that have Internet, restricts employees use and monitor what they actually do on the Internet.

However, just a few of the organisations have written Internet use policy, which shows that the articulation and implementation of clear written policy is still lagging. The study also shows that only few of the organisation that have Internet use policy have complied and disciplined its employees on Internet misuse.

The commonly encountered problems in the organisations were excessive chatting that is non-work related and accessing pornography sites at work.

a) Suggestions for further studies

The following recommendations are made for further studies:

1. This study basically considered the use of Internet in organisations in Ibadan. More studies are needed to explain the pattern of Internet adoption by organisation as there are different adoption stages to technology.
2. This study is an organisational study that focused on employers alone, future study can focus on both employees and employers so that the perception of both side can be known.
3. More so, this study was not anchored on any empirical theories, future studies can look into empirical theories to understand the antecedents of Internet abuse, so that more variables can be used to gather data.
4. Lastly, it is recommended that further study on the impact of Internet use on employees' productivity should be carried out.

References Références Referencias

1. Adams, H., Scheuing, S.M. & Feeley. S.A. (2000) E-mail Monitoring in the Workplace: The Good, the Bad and the Ugly, *Defense Counsel Journal*, 67:1, pp. 10-14
2. Adebayo, A. O. (2007). An Investigation of the Use of ICT in the Nigerian Construction Industry. Retrieved January 24, 2011 from *http://www.itcon.org/2007/18*
3. Alese, B. & Owoyemi, S.(2004) Factor Analytic Approach to Internet Usage in South Western Nigeria. *Journal of Information Technology Impact*, Vol. 4, No. 3, pp. 171-188
4. Ali, A. & Denga, D. I. (1989).*An introduction to research methods in statistics in education and social sciences*. Calabar, Nigeria: Rapid Education publisher, pp. 25-36.
5. Alge, B. J. (2001). Can corporate security, privacy coexist? Retrieved June 30, 2011 from www.newswise.com/articles/2001/5/privacy2.pur.html
6. Awoleye, O.M., Siyanbola, W.O., & Oladipo, F.O. (2008). Adoption Assessment of Internet Usage amongst Undergraduates in Nigeria Universities- A Case Study Approach*. Journal of Technology Management and Innovation (JOTMI Research Group)* Santiago Chile. Vol. 3(001) pp. 84-89
7. American Library Association (2005) "Survey of Internet Access Management in Public
8. Libraries." Retrieved December 13 2010 from http://www.lis.uiuc.edu/gslis/research/Internet.pdf
9. Anonymous (2000). E-business or Bust: The Impact of the Internet/Net Effects, *Sales and Marketing Management, 15:2,* pp. 63-65.
10. Anonymous (2001).Internet Abuse is on the Increase, *Management Services*, 45:6, 2001, p. 3.
11. Bus. J. (1998). *The Secret Agents of Fortune*. Retrieved June 12, 2011 from http://www.secure-data.com/art9.html
12. Camille L. H. (2002) *Methods and Extent of Employer Use of Electronic Monitoring and Surveillance*, Employee Privacy Law Retrieved June 12, 2011 from http://www.amanet.org
13. Caroll, W. R (2007) Electronic Monitoring in the Workplace: *A Review and Discussion about Future Trends. The workplace Review, 4, 2 3-7:* Retrieved on January 12, 2011 from *http://www.smu.ca/-academic/sobey/workplacereview/Nov2007/WPR novIsuue.pdf*
14. Cochran, W.G. (1987). *Sampling techniques*. Wiley Eastern Limited, p.268
15. David, D., David, F. & Marczyk, G. (2005).*Essentials of research design and methodology*. New Jersey: John Wiley & Sons Inc., 18p.
16. Davies, R. A. (2001) *Cybers lacking: Internet abuse in the workplace.* Retrieved July 20, 2011 from http://www.Internetaddiction.ca/cyberslacking.html
17. Dancaster, L. (2001) "*Internet Abuse: A Survey of South African Companies*" ILJ Volume 22 p. 862
18. Deisz, J. (2005). Internet filtering and how it affects security, efficiency and thriving in Norwegian Companies. *Msc Thesis published with Royal Institute of Technology (KTH), Stockholm.* Retrieved 13 December, 2010 from http://www.nislab.hig.no
19. DeTienne, K.B. & Abbott N.T. (1993) Developing an employee centred electronic monitoring system. *Journal of Systems Management*, Volume 44(8) p.12.
20. Elise M. B., (2002) Competing Interests in the Post 9-11 Workplace*: The New Line Between Privacy and Safety*, 1317 Practicing L. Inst./Corp. 303
21. Erah, P.O, & Dairo, E.A.(2008) Pharmacy Students Perception of the Application of Learning Management System in Patient-Oriented pharmacy Education: University of Benin Experience. *International Journal of Health Research, June 2008*. Vol. 1(2) pp. 63-72.
22. Forrester Research, Inc., (2007) "Internet risk management in the Web 2.0 world," September, 2007

23. Fox News (2000) Employers Crack Down on Internet Abuse. *FoxNews.com* November 5, 2000 Retrieved February 12, 2011 *http://www.foxnews.com/scitech/-110500/survwillance.sml*
24. Gahtan, A. (2002). Monitoring Employee Communications. *The Cyber law Encyclopedia*. Retrieved January 06, 2011 from *http://www.gahtan.-com/alan/articles/monitor.htm*
25. GFI WebMonitor (2005) http://www.gfi.com/-webmonitor/Retrieved December 11, 2010.
26. Griffiths, M. (2000). Does Internet and computer ''addiction'' exist? Some case study evidence. Cyberpsychology and Behavior, Volume 3(2), 211–218.
27. IBM (2004) "Global Business Security Index 2004". Retrieved January 24, 2011 from *http://www1.ibm.-com/services/us/index.wss/rs/imc/a1008866?cntxtId =a1000400*
28. International Data Corporation (IDC) (2004) Worldwide Leader in Web Filtering Expands into Web. Retrieved January 17, 2011 from http://www.idc.com/getdoc.jsp?containerId=32218
29. Internet based encyclopaedia. Retrieved January 07, 2011 from *http://www.wikipedia.org*
30. Jason, P. (1997). Banking on computers. *African Business* Volume 219, 40-42.
31. Lane, F. S. (2003). The Naked Employee: How Technology Is Compromising Workplace Privacy. *New York: American Management Association. 2003. Print.*
32. Lehr, B. & Lichtenberg, F.(2000). Information Technology and Its Impact on Productivity: Firm-level Evidence from Government and Private Data Sources 1977-1993, *Canadian Journal of Economics, 32:2, pp. 335-362*
33. Leung, L., & Wei, R. (1999). The gratifications of pager use: sociability, information-seeking, entertainment, utility, and fashion and status. *Telematics and Informatics* 15(1), 253–264.
34. Leung, L., & Wei, R. (1999). Who are the mobile phone have-nots? *New Media & Society, 1*(2), 209-226.
35. Leung, L., & Wei, R. (2000). More than just talk on the move: Uses and gratifications of the cellular phone. *Journalism and Mass Communication Quarterly*, 77(2), 308-320
36. Leung, L. (2001). College student motives for chatting on ICQ. *New Media and Society* 3(4), 483–500.
37. Leung, L. (2002). Loneliness, self-disclosure, and ICQ (''I Seek You'') *use Cyber Psychology & Behavior* 5(3), 241–251.
38. Lim, E. and Vivien, G (2002). The IT way of loafing on the job: cyberloafing, neutralizing and organizational justice. *Journal of Organizational Behavior*. 23, 675-694. Wiley InterScience (www.interscience.wiley.com).
39. Lippert, S.K. (2004). The Effect of Trust on Personal Web Usage in the Workplace. *A guide to Effective Human Resources Management.* Information Science Publishing, USA. 2004, pp 178-200 Retrieved on 05 December, 2010 from http://www.idea-group.com
40. Lyold, P.C (1967). *The City of Ibadan*. Cambridge University Press. ISBN 978-0521112178.
41. Marsan, C.D (2000). "Employee Study Cites Rampant Internet Abuse, *Network World*, 17:17, p. 38
42. Madueme, I. S. (2010) Evaluation of the Impact of Information Communication Technology on Banking Efficiency Using the Transcendental Logarithmic Production function and Camel Rating. *International Journal of Engineering Science and Technology*, Vol.2 (1), 2010, 1-6.
43. Net Monitoring Survey (2000) *Informationweek.com* 2000 Volume 805 pp211.
44. Ndukwe, E. (2005), "ICT Infrastructure: An Essential Foundation for Implementing the WSIS Process in Nigeria", *e-Nigeria Annual National Conference*, 28-30 June, Abuja, Nigeria.
45. Nwagwu, W. E. (2007). The Internet as a source of reproductive health information among adolescent girls in an urban city in Nigeria*. BioMed Central Public Health* 7(2), 2-13.
46. Olatokun, W. M. & Adeboyejo, O.C. (2009) Information And Communication Technology Use By Reproductive Health Workers In Nigeria: State Of The Art, Issues, and Challenges. *An Interdisciplinary Journal on Humans in ICT Environments*. Vol. 5(2), November 2009, pp. 181- 207. Retrieved on January 26, 2011 from http://www.humantechnology.jyu.fi
47. Omolase, C. O., Ihemedu, C. O., Ogunleye, T. O., & Omolase, B. O. (2010). Use of Internet for Health Information amongst Medical Practitioners in a Nigerian Community. *TAF Preventive Medicine Bulletin, 2010*. Vol. 9(2):93-98
48. Orhuozee, E. (2002, August), More Promising E-Governance Strides in Nigeria, *PC World West Africa*, IT Media Group, 6-7.
49. Otokhine, E. (2002, January). Nigeria Moves Forward with E-Banking, *PC World West Africa*, IT Media Group, 4-7
50. Overly, M.R. (1999) E-Policy: How to Develop Computer, E-mail, and Internet Guidelines to Protect your Company and its Assets, *NY: American Management Association (AMA).*
51. Papacharissi, Z. & Rubin, A. M. (2000). Predictors of Internet use. *Journal of Broadcasting & Electronic Media, 44*(2), 175-196.
52. Paul E. H. & Ibrahim C. M.., (1996). E-Mail, Electronic Monitoring, and Employee Privacy *International Journal of Engineering Science and Technology*, Vol.23(2) p. 893- 897

53. Peters, O. (2007). *Social Psychological Determinants of Mobile Communication Technology Use and Adoption: A Comparison of three Models to Explain and Predict Mobile Communication Technology Behavior* (Thesis), University of Twente, pp. 23-27.
54. Privacy Rights Clearing House web site, Retrieved January 23, 2011 from http://www.privacyrights.org/fs/fs7-work.htm
55. Raposa, P., & Mujtaba, B. (2003). The Ethics of Employee Monitoring: What You Need to Know. *Business, Trust and Responsibility* Conference, 11-13 April, 2003. Orlando, Florida. http://www.idc.com/getdoc.jsp?containerId=32218
56. Secure Computing (2004) Secure Computing filtering overview. Retrieved January 26, 2011 from http://www.securecomputing.com/index.cfm?skey=274
57. Seltzer L.,(2000). Monitoring Software. *PC Magazine* 2000 Volume 20(5) pp26-28.
58. Schulman, A. (2000). Privacy Foundation web site, Retrieved. January 23, 2011 from http://www.undoc.com/onworsurproj.html
59. Silva, D. (2001). "Companies Take Steps to Combat Internet Abuse," *Puget Sound Business Journal*, Seattle, vol. 22(23), 2001, pp. 5-7
60. Simmers C.A. & Anandarajan, M. (2004). Convergence or Divergence? Web Usage in the Workplace in Nigeria, Malaysia and the United States*. Personal Wed Usage in Workplace: A guide to Effective Human Resources Management.* Information Science Publishing, USA. 2004, pp 178-200 Retrieved on 05 December, 2010 from http://www.idea-group.com
61. Singh, M. A. (2004) Managing employee Internet abuse. *South African journal of Information management* Vol.6(3) September 2004
62. Society of Human Resource Managers (2002). "Technology and Privacy Use."Retrieved June 23, 2011 from http://www.shrm.org/trends/visions/default.asp?-page=0300c.asp
63. Sonny S. (2002) Computer Monitoring: Benefits and Pitfalls Facing Management, *Information & Management*. Volume 39, p.553, 556-557.
64. SR. (2000). Snoop at Your Peril. *PC Magazine* 2000 Volume 19(17) pp86.
65. Stratopoulos, T. & Dehning, B. (2000). "Does Successful Investment in Information Technology Solve the Productivity Paradox?" *Information & Management*, 38:2, 2000, pp. 103-117.
66. Sullivan, K.B. (1996). *Web Monitoring and Filtering Programs Promote Productivity* PC-Week, 13:50, 1996, pp. 21-22.
67. Swanson S. (2001), Beware: Employee Monitoring Is On The Rise. *Informationweek* 2001 Voulme851 pp57-58.
68. Telenor (2004) *"IT sikkerhet -Trender og utvikling i 2004"* Retrieved on December 24, 2010 from http://www.telenor.no/bedrift/sikkerhet/news_show.php?news_id=35
69. The Central Intelligence Agency (CIA) 2000 World Factbook (2000). Retrieved January 24, 2011 from: http://www.cia.gov/cia/publications/factbook/index.html.
70. Thompson, J. (1994). Here come the giants. *African Business*, Vol.190(2), pp. 42.
71. United Nations Publication(2007) Internet Use For Business Development: An Introductory Set Of Training Modules For Policymakers. Bangkok 2007
72. Urbaczewski A. (2000). Monitoring Strategies for Internet Technologies. *Personal Web Usage in Workplace: A guide to Effective Human Resources Management.* Information Science Publishing, USA. 2004, pp 178-200 Retrieved on 05 December, 2010 from http://www.idea-group.com
73. Vanscoy K., (2001), What Your Workers Are Really Up To. *Smartbusinessmag.com* 2001 Volume 15(9) pp50-54.
74. Villeneuve, N. (2008) Breaching Trust: An Analysis of Surveillance and Security Practices on China's TOM-Skype Platform, Information Warfare Monitor/ONI Asia. Retrieved June 30, 2011 from http://www.nartv.org/mirror/breachingtrust.pdf.
75. Wallace P. (2004), The Internet in the Workplace: How new technology is Transforming Work. Cambridge University Press. USA Retrieved on January 31, 2011 from http://www.cambridge.com
76. Websense (2005), Homepage of Websense Internet filtering company. Retrieved January 25, 2011 from http://www.websense.com
77. Wei, L. & Zhang, M. (2008). The Adoption and Use of Mobile Phone in Rural China: A Case Study of Hubei, China. *Telematics and Informatics* 25, 169-186.
78. Wilder C, (2001) A Question of Ethics. *Informationweek.com* 2001 Volume825 pp39-50.
79. World Internet Users. *InternetWorldStats.com.2010.* Retrieved December 18, 2010 from http://www.Internetworldstats.com/stats.htm
80. Young, K. S. & Case, C.J. (2003) Employee Internet abuse: risk management strategies and their Effectiveness, *Proceedings of the American Society of Business and Behavioral Sciences, Las Vegas,* February 21, 2003, p 1688-1694
81. Yulihasri, Ramayah T., Norzalila J., & Amlus I., (2006) Use and Misuse of the Internet in the Malaysian Workplace: Preliminary Findings from an Exploratory Study IAMOT, 2006
82. Zuckerman, E. (2010) Intermediary Censorship in Access controlled, in Deibert, R., Palfrey, J.,Rohozinski, R. And Zittrain, J. (Eds) *The Shaping of Power, Rights and Rules in CyberSpace*, the MIT press, pp 71-85

This page is intentionally left blank