Annals of Library and Information Studies
Vol. 58, September 2011, pp. 282-294

Internet access, use and monitoring policies in Botswana organizations

Wole Olatokun[1] and Betty Moremedi[2]

[1]Africa Regional Centre for Information Science (ARCIS), University of Ibadan, Nigeria, Email: woleabbeyolatokun@yahoo.co.uk
[2]Department of Library and Information Studies, Private Bag 0022, University of Botswana, Gaborone

The study determines the level of access to the internet in various organizations in Botswana. It investigates the problems brought about by the misuse of internet facilities in the workplace and the measures or policies put in place to monitor internet use. It also reports the use, restrictions and monitoring of internet facilities by organizations to their employees. Survey research design was adopted and questionnaire was used for data collection. It was administered across 113 organizations in Gaborone, the capital city of the Republic of Botswana. The data was analyzed using the SPSS software. Findings revealed that although majority of the organizations monitor employee internet use, less than half had an internet use policy in place. Also, majority provide access to all employees with the least from the public administration/Government. More than three quarter of them do not monitor and review websites connections, some monitor and review websites connections for all the employees while a few others monitor and review websites connections for selected job categories. Majority restricted or blocked pornographic and online gaming sites while news sites enjoyed free access. All the public sector organizations indicated having a written policy on internet use but majority of research organizations had no policy. The study recommends that organizations should produce and implement written policies on internet use and inform employees about such policies and come up with measures to monitor employee use of internet in the workplace.

Introduction

Worldwide, internet usage has continued to grow. Based on the 2005 estimates, penetration in world regions varied from 1.5 percent in Africa to 67.4 percent in Northern America. In that same span, other industrialized nations probably reach just below 75 percent usage (Cole[1] cited in Anandarajan et al[2]). Bacal[3] commented that when it was written down originally, the internet was less available, and less essential, but since then, almost every workplace has employee access to the internet and email and with the result, the issue of abusing internet access at work has escalated. TechGenix Ltd.[4] noted that the internet has become a prime business tool and workplaces the world over are rapidly becoming wired. It facilitates communication, enhances collaboration without the need for travel or expensive phone bills, and improves productivity in organizations. However, a wired workplace can find its productivity hampered due to employees abusing internet access. The internet is vast and the temptation to surf the net out of personal interest while at work proves to be a highly alluring proposition for many.

Recognizing the criticality of the internet, researchers began a longitudinal project in 2006 at the University of Southern California's Annenberg School Center for Digital Future. The Center has been annually collecting data regarding internet users and nonusers, the ways people use it, and its effects on their online and offline lives. The internet is the most significant source of information and its use increases productivity. Simultaneously, there were troubling transformations such as increase in deviant internet behavior, varying degrees of severity from cyber loafing[5]. The practice of censorship, along with surveillance of people using the internet are often viewed as activities performed by states and was the subject of a study by the Open Net Initiative (Deibert et al[6] cited in Alampay and Hechanova[7]). The study used various perspectives to examine the political, legal, social, and cultural contexts of internet filtering in some countries and its implications for communities that rely on internet technologies for communicating their mission. Critical to this approach was the role that internet service providers played, as directed by government authorities, in the filtering process.

Other studies[8-11] have looked at other points in the network, where internet filtering occurs. Zuckerman[12] cited in Alampay and Hechanova[13], for instance,

looked at filtering or censorship performed by online service providers (OSPs) for services such as social networking sites, blogs and websites, and refers to these as a form of intermediary censorship. Another point in the network in which this is also done is at the organizational level, whereby offices, schools, libraries and businesses are also able to filter and monitor internet use. Bacal[14] stated that more and more government organizations are installing internet access for staff, and the common questions are how do one regulate usage without making the technology useless? In fact, what degree of regulation is appropriate? In trying to answer these questions he submitted that the extreme cases of abusive behavior such as accessing pornographic materials, harassing other internet users, or conducting political activities during work hours may need stronger methods, including monitoring of log files, followed by appropriate disciplinary actions. Anandarajan et al[15], maintain that organizations are now at the point which employee's productivity and knowledge-asset management has become a major workplace concern and without proper internet management strategies, employees can misuse it and spend their work time on personal activities.

In most organizations in Botswana, users are given access to the internet which is possibly meant mainly for work related activities. Organizations are now at the point where employee's productivity and knowledge-asset management has become a major workplace concern. Without proper internet management strategies, employees can misuse internet, and spend their work time on personal activities. But in most cases, one finds occasions when employees turn it into their personal uses instead of for work activities. According to use gratification theory, people use internet to fulfill some need (Newhagen and Rafaelli[16] cited in Anandarajan et al[17]. Computer viruses spread due to downloaded material from the internet and some computer systems and networks are exposed to threats, attack and vulnerability. The community sites e.g. sites such as facebook, hi5 and others are the ones that a lot of people visit most of the time, so this slows down the internet, and hinders some work related activities which should be done through the network. Productivity in the workplace also becomes low in organizations that rely in the use of internet because the system would be slow and at times, it crashes. Some previous studies[18-21] have put more emphasis on internet use, access and monitoring in the workplace based on the user/employee's perspective.

Review of literature

The development of new communication and information technologies has revolutionized the way that business is conducted[22]. In the U.S., more than 130 million workers send out 2.8 billion e-mail messages each day[23]. On the one hand, e-mail, the internet, and other new technologies provide an opportunity to improve productivity and profitability, but on the other hand, they can pose a realistic threat to organizational effectiveness and actually impede it. For instance, business e-mails can be concise, quickly composed, and instantly transmitted, thereby improving organizational effectiveness when they replace cumbersome, time-consuming formal memos and letters. Unfortunately, e-mail can also impede organizational effectiveness when employees waste hours e-mailing family and friends using their company e-mail accounts. The internet, like e-mails, can also serve to improve organizational effectiveness when used to conduct company-related e-commerce and business-to-business (B2B) transactions. Conversely, the internet can impede organizational effectiveness, when employees sit and waste hours surfing the Web, shopping for personal items, and downloading files and programs for personal use[24]. One survey found that one out of every eight American workers spend two or more hours per day writing and reading personal e-mails and using their work-based internet connection for non-work related activities[25]. Another survey[26] found that more than 90 percent of American workers acknowledged that they used the internet for personal purposes during work hours and 84 percent said that they used their employer-provided e-mail accounts to send and receive personal e-mails[27]. These new technologies may not only threaten the organization indirectly (via reduction in worker productivity) but also directly because of employees' inadvertent or deliberate misuse[28].

A 2004 American Management Association (AMA) survey on workplace e-mail and instant messaging (IM) found that of 840 companies surveyed, 13 percent have faced workplace lawsuits that were triggered by employee e-mail[29]. New technologies have not only provided employers with new reasons to monitor employees' behavior, these technologies

have also provided organizations with new methods to carry out employee monitoring. Technological advances in global positioning systems (GPS) and biometrics enable organizations to track accurately and cost-effectively worker movements in the office, in the field, and on the road[30-32]. Using devices such as GPS sensors in company-provided cell phones and cars, infrared LED ID badges, and biometric touch-pads, employers can know whether a trucker is deviating from a prescribed route, whether a receptionist is taking too long for a lunch break, whether an outside salesperson really is calling on customers, and even whether a food handler has washed his hands after going to the bathroom[33-34]. Thanks to dramatic improvements in video and audio technologies, organizations can conduct efficient, unobtrusive, and comprehensive surveillance of their workers[35].

With the proliferation of e-mail and internet-related technologies in the workplace, there has also been a dramatic expansion of technologies to monitor employees' use of these technologies[36]. Electronic monitoring programs such as *Investigator, Black Orifice, Mail Marshall, Websense, Survey Suite, Spector,* and others enable employers to track employee keystrokes, comb through employee e-mails, review employees' computer files, see what websites employees have visited, determine how long an employee stays online, block employee visits to forbidden websites, and perform various other monitoring and surveillance functions. Some analysts note that electronic monitoring in the workplace is rapidly becoming as ubiquitous as electronic communications and argue that employees have come to expect it (if not accept it)[37]. Nolan[38] argues "by now every sensible employee knows, or should know, that employers do or at least may use all of the tools of modern technology to supervise and direct them" (p. 207). Notwithstanding this claim, recent employee surveys and studies of employee responses to electronic monitoring suggest that many employees are surprised and alarmed about the extent of electronic monitoring of their workplace activities, with a significant percentage quite convinced that it is illegal for employers to engage in such monitoring[39-43]. Employees may perceive electronic monitoring of their behavior as an unwarranted invasion of their right to privacy and as fundamentally unfair[44-48]. In addition to these privacy concerns, a considerable body of research indicates that in some cases electronic monitoring may lead to increased levels of employee stress, worsening employee health, and declining levels of productivity[49-52].

According to Lease & Gordon[53], the reasons for electronic monitoring can be categorized as falling under "legitimate business concerns". However, some analysts argue that in some cases, employers may have less than noble hidden motives for monitoring, including union busting/avoidance, morality (e.g., suppose an employer wants to ensure that none of its employees are homosexual), or outright curiosity (e.g., since there are few restrictions on employer monitoring, employers may seek to indulge their curiosity about employee behavior and activities)[54]. A review of literature by Lease & Gordon[55] suggests that, in general, the stated reasons for electronic monitoring by employers, can be covered under four categories: 1) productivity/profitability; 2) security; 3) legal liability/compliance; and 4) employee performance review/feedback[56-59].

From the employee perspective, their primary objection to electronic monitoring is that it constitutes a breach of privacy[60]. They may also object on the grounds that monitoring is a threat to their health and/or that it is unfair and unethical[61-68]. Employees' health objections to electronic monitoring, especially to electronic performance monitoring with respect to specified performance quotas and goals, concerns the charge that it leads to increased levels of workplace stress, lower quality of work life, and resultant adverse impact on employee health. There is considerable evidence that stringent monitoring and aggressive performance quotas do in fact lead to an increase in stress-related disorders among monitored employees[69-71]. A direct connection between this research and possible adverse health effects of electronic monitoring of employee e-mail and internet use, in the absence of performance goals or quotas, is uncertain.

Most of the existing research on employee perceptions of electronic monitoring focuses on employees' privacy concerns. It is an oversimplification to say that employees unilaterally view electronic monitoring in the workplace as an invasion of privacy. Most employees do believe – notwithstanding any legal facts – that they have a "right to privacy" in their workplaces[72]. Employees do not believe that employers have an unfettered right to intrude upon their privacy, or, more specifically,

employees generally believe that it is *illegal and unethical* for employers to intrude into employees' "zone of privacy" regardless of how they may define it[73-75]. This does not imply, however, that employees do not think that employers have some right of their own to monitor employees' activities in the workplace. Research suggests that the degree to which employees accept monitoring or view it as an intrusion upon their privacy depends upon a number of factors including what is being monitored, the purpose/justification of monitoring, the usefulness of monitoring, employees' awareness/knowledge of monitoring, and the "fairness" of monitoring (i.e., issues related to procedural justice).

The dearth of studies in Botswana that address the problem of employees monitoring in the workplace underscored the need for this study. Focusing on an analysis of employers' electronic monitoring of employee e-mail and internet behavior, this study set out to find out on what basis the organizations in Botswana use internet and regulate its use, identify the problems brought about by the misuse of internet facilities, and find out if some organizations have measures or policies put in place to monitor internet use in their workplace.

Objectives of the study

- To find out the extent to which, organizations in Botswana provide and regulate internet use;
- To determine the pervasiveness of internet/computer monitoring among organizations; and
- To examine if organizations in Botswana have formal policies in place to regulate the use of internet and computer facilities and how are these policies made known to employees.

Methodology

The study adopted the survey research design approach. It was conducted in Gaborone, the capital city of the Republic of Botswana in selected organizations that mostly rely on the internet for their services including communication with their customers and for attracting clients or customers online through online advertising. These organizations were grouped into seven strata namely: Public Administration /Government, Banking/ Financial Services, Research, Manufacturing, Wholesale/Retail and Education/School. A sample of 113 organizations was selected using stratified random sampling technique as follows: 15 organizations from Public Administration/ Government, 21 from Business/Professional Services, 18 from Banking/Financial Services, 8 from Research, 9 from Manufacturing, 12 from Wholesale/ Retail and 19 from Education/School.

Data were collected using a structured questionnaire because it has standardized answers that make it possible to compile data for easy analysis. It consisted of five sections: Section A collected data about the organization's profile, section B elicited data on internet access and use in the organizations and section C gathered data on internet monitoring/usage in the organizations, section D collected data about respondents' use of internet, and section E gathered data on policy compliance and discipline. Prior to the administration of the questionnaire, it was examined by experts in internet research and their comments were used to arrive at the final version. A Cronbach alpha reliability co-efficient of $\alpha = 0.89$ was achieved. A total of 125 copies of questionnaire were hand delivered across the sampled organizations in the month of March 2010. The personnel, in most cases the head/proprietor of each organization filled (self-report) the data in the questionnaire. Organizations with less than fifty employees were the largest with 51 respondents (45%), followed by organizations with 101-500 employees with 27 respndents (24%). Organizations with 501-1000 and above 1000 employees were the least represented with 8 respondents (7%) each. Also, private organizations were in the majority with over fifty percent followed by government sector organizations with 20 respondents (18%). For profit organizations with 11 respondents (10%) and non-profit organizations with 7 respondents (6%) followed in that order respectively. Organization types included: business/professional services organizations 21(19%), followed by educational/school 19(17%) and then banking/financial services organizations 18(16%). The least participants were from research organizations 8(7%).

Analysis

Organization type and internet access

The respondents were asked to indicate who has internet access in their organizations and the extent of internet access. The results are presented in Table1.

The results in Table 1 showed that majority of organizations provide access to all its employees (76), followed by those that provide access only to manager/supervisor (19) and the least were the organizations which provide access to its employees depending on the job (18). Across the organization types, educational/school sector are in the majority of those who provide access to all its employees (18), followed by business/professional service organizations (17). The least were wholesale/retail (4) and manufacturing (1) respectively. The results also revealed that among the organization types surveyed, the majority of organizations provide internet access to its employees but with some restrictions (69), for which the organization with the largest number to be providing access with some restrictions were banking/financial services organizations (15), and educational/school (15). On the organizations with complete access (43), business/professional services organizations had the majority with (15) and the least was public administration/government. This shows that public sector organizations do not provide complete access to their employees.

Organization and nature of restriction

The respondents were asked to indicate the nature of restrictions that their organizations provide for their internet access. The results are presented in Table 2.

Results in Table 2 showed that the majority of organizations block some applications/sites (57) with banking/financial services organizations having the largest number of applications/sites blocked (72%), followed by education/school (71%).

Table 1—Organization type and internet access

Who has access?

Organization type	All	Manager / Supervisor	Depending on job	Total
Business/ Professional services	17	3	1	21
Banking / Financial Services	12	5	1	18
Research	7	0	1	8
Manufacturing	1	3	5	9
Wholesale/Retail	4	4	4	12
Public administration / Government	11	1	3	15
Educational / School	18	0	1	19
Others	6	3	2	11
Total	76	19	18	113

Extent of access

	Complete access	Completely no access	Some restrictions	Total
Business/Professional services	15	1	5	21
Banking / Financial services	3	0	15	18
Research	3	0	5	8
Manufacturing	6	0	3	9
Wholesale / Retail	3	0	9	12
Public administration / Government	2	0	13	15
Educational / School	5	0	14	19
Others	6	0	5	11
Total	43	1	69	113

Table 2—Nature of restrictions across organizations

	Some applications/sites are blocked		Some sites are blocked during work hours but are accessible during breaks/after office hours		Only some computers have access		Accessible sites are dependent on the nature of the job		Blocked sites can be accessed if permission is requested by the systems administrator		Other restrictions	
	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes
Business/Professional services	15	6	19	2	21	0	19	2	20	5 1	21	0
Banking/Financial services	5	13	12	6	16	2	16	2	12	6	18	0
Research	3	5	8	0	8	0	7	1	8	0	8	0
Manufacturing	7	2	8	1	8	1	9	0	9	0	9	0
Wholesale/Retail	7	5	10	2	9	3	9	3	10	2	11	1
Public administration/Government	6	9	11	4	13	2	12	3	8	47 7	15	0
Education/School	6	13	12	7	17	2	18	1	13	60 6	18	1
Other	7	4	7	4	11	0	7	4	8	3	11	0
Total	56	57	87	26	103	10	97	16	88	25	111	2

Pattern of monitoring across organization types

The respondents were asked if their organizations monitor and review websites connections, and to indicate the pattern of monitoring if it was practiced. The results are presented in Table 3.

The results in Table 3 revealed that majority of organizations do not monitor and review websites connections in their organizations (49), followed by the organizations which monitor and review websites connections for all the employees (34), while the least were those organizations which monitor and review websites connections for selected job categories (25). Across the different organization type, majority of the organizations which do not practice this monitoring are the business/professional services (12), followed by wholesale/retail organizations (7) and the least were public administration/government (2).

Availability of written policy on internet use across organization types

The respondents were asked if they have a written policy on internet use in their organizations. Results showed that majority of the organizations have a written policy on internet use (48). Public administration/government organizations had a majority of respondents who indicated availability of a written internet use policy with 100 percent. This was followed by the Business/Professional service organisation with (67%). The least was research organisation (14%).

Who monitors internet use across the organizations?

As part of the survey, the participants were asked to specify who monitors internet in their organizations. The results are presented in Table 4.

The results in Table 4 revealed that the majority of organizations used a dedicated MIS Staff/Systems Administrator 45(40%) to monitor internet use, followed by those that used software 28(25%). Organizations that had immediate supervisors of the employees to monitor internet use had the least number of respondents with 11(10%).

What are being monitored in internet use across the organizations?

The respondents were also asked to indicate what aspect of internet use was monitored by their organizations. The results are presented in Table 5.

The results presented in Table 5 showed that majority of 54 (48%) organizations monitor matter/content accessed , followed by those who monitor time spent on the internet [27 (24%)]. The least were those that monitored personal blogs of employees (and applicants) [13(12%)].

Table 3—Pattern of monitoring across organizations

Organization type	All employees	Selected job categories	Not practiced	Total
Business /Professional services	5	3	12	20
Banking/Financial services	6	6	5	17
Research	1	1	6	8
Manufacturing	1	2	6	9
Wholesale / Retail	2	3	7	12
Public administration / Government	10	1	2	13
Educational / School	5	7	6	18
Others	4	2	5	11
Total	34	25	49	108

Table 4—Who monitors internet use across the organizations?

	No		Yes		Total	
	Frequency	Percent	Frequency	Percent	Frequency	Percent
The immediate supervisor	102	90.3	11	9.7	113	100.0
A dedicated MIS Staff/System Administrator	68	60.2	45	39.8	113	100.0
Software	85	75.2	28	24.8	113	100.0
Others	95	84.1	18	15.9	113	100.0

Table 5—What are being monitored in internet use across the organizations?

	No		Yes		Total	
	Frequency	Percent	Frequency	Percent	Frequency	Percent
Time spent on the internet	86	76.1	27	23.9	113	100.0
Matter/content accessed in the internet	59	52.2	54	47.8	113	100.0
Personal blogs of employees (and applicants)	100	88.5	13	11.5	113	100.0
Others	104	92.0	8	7.1	113	100.0

Use of blocking software and restricted/blocked sites

The respondents were asked if their organizations use blocking software to prevent internet connections to unauthorized/inappropriate websites and to specify the kinds of sites that were blocked. The results showed that majority of the organizations used blocking software to prevent internet connections to unauthorized/inappropriate websites 64(57%). Table 6 shows the types of blocked sites in the organizations.

The results in Table 6 showed that majority of the organizations restricted or blocked pornography sites 70(62%), followed by those that had blocked or restricted online gaming sites 52(46%). The least blocked sites were News (Inquirer, GMAnews, NYTimes, etc.) 109(97%), followed by Online mail services (Yahoo mail, Gmail, Hotmail, etc.) 106(94%) and blog sites 97(86%) respectively. This shows that the majority of organizations use/value news sites and online mail services sites for their work.

Email use in the organisations

The respondents were asked if their organizations store and review employee email messages, and how they do it, if they monitor. The results revealed that the highest number of respondents (66%) indicated that their organizations store and review email messages of all their employees. This was followed by those that do not practice the monitoring of computer files 19(17%), and the least were those that monitor for selected job categories 17(15%).

Table 6—Restricted/blocked sites

	No		Yes		Total	
	Frequency	Percent	Frequency	Percent	Frequency	Percent
Downloading of video/pictures/music (e.g. YouTube)	75	66.4	38	33.6	113	100.0
Social networking sites	69	61.1	44	38.9	113	100.0
Pornography sites	43	38.1	70	61.9	113	100.0
Online gaming sites	61	54.0	52	46.0	113	100.0
Yahoo Messenger!	99	87.6	14	12.4	113	100.0
Skype	90	79.6	23	20.4	113	100.0
Blog sites	97	85.8	16	14.2	113	100.0
News (Inquirer, GMAnews, NYTimes, etc.)	109	96.5	4	3.5	113	100.0
Online mail services (Yahoo mail, Gmail, Hotmail, etc.)	106	93.8	7	6.2	113	100.0
Others:	109	96.5	4	3.5	113	100.0

Table 7—Policy on personal internet use

	No		Yes		No response	Total	
	Frequency	Percent	Frequency	Percent		Frequency	Percent
Does your organization have a written policy governing personal use of email?	78	69.0	33	29.2	2(1.8)	113	100.0
Does your organization have a written policy governing personal use of the internet?	72	63.7	40	35.4	1(.9)	113	100.0
Does your organization have a written policy governing personal use of instant messaging?	88	77.9	23	20.4	2(1.8)	113	100.0
Does your organization have a written policy governing the operation of personal websites on company time?	71	62.8	39	34.5	3(2.7)	113	100.0

Organizational policy on email use

The respondents were asked to indicate whether there was an organizational policy on email use in their organizations, and if the employees were informed of such policies.

It was found that majority [84(74%)] of the organizations do not have policies that says when monitoring of email accounts could be done. Further, those organizations that have a policy of monitoring employee email accounts, 40% of the respondents stated that they were informed of the organization's policy of monitoring emails.

Computer surveillance

The respondents were asked if their organizations store and review employee's computer files, and how they do it. The results revealed that the highest number of organizations that practiced computer surveillance was those organizations that store and review employees' computer files for all their employees 77(68%), followed by those that do not practice the monitoring of computer files 17(15%), and the least were those that monitor for selected job categories 16(14%). The results also showed that for those organizations that monitor employee's computer files, the majority [17(15%)]store and review employee's computer files routinely, followed by those that their monitoring was ongoing 11(10%),and the least were those that their monitoring was specified 10(9%).

Organizational policy on personal use of internet

As part of the survey, the respondents were asked if they have organizational policies on personal use of internet. The results are presented in Table 7.

The results in Table 8 show that majority of the organizations [40(35%)] had a written policy governing personal use of the internet, followed by those organizations [39(35%)] that had a written policy governing the operation of personal websites on company time respectively. The least were those that had a written policy governing personal use of email [33(29%)] and those that had a written policy governing personal use of instant messaging [23(20%)]. The results also show that a lot of organizations do not have organizational policies on personal use of internet; the highest numbers are for those organizations that do not have policies as compared to those that have policies on personal use of internet.

Disciplining employees for misuse of email and internet facilities

The respondents were asked if their organizations had ever disciplined an employee for misuse or private use of office internet connections/facilities, and to indicate the form of discipline that was taken against such employee. Results showed that majority had never disciplined their employees on the misuse or private use of office internet 87(77%). They also showed that those organizations that had disciplined their employees, the majority used formal reprimand/warning 14(12%) as the form of discipline taken against an employee, followed by dismissal 7(6%). The least used form of discipline was informal reprimand/warning 4(4%). Concerning the disciplinary measures on private email misuse, the results showed that majority of the organizations had never disciplined their employees for company email misuse 96(85%). The results also showed that those organizations that had disciplined their employees, majority used formal reprimand/warning 7(6%) as the form of discipline taken against an employee, followed by informal reprimand/warning 4(4%).The least form of discipline used was dismissal with 1(.9%).

Discussion

The findings showed that a lot of organizations in Botswana provide internet access to their employees in the workplace. They do so to make organizational business and communication easier. Some organizations especially in the private sector use internet to operate their businesses and provide professional services across the country to enable communication with other business branches or their stakeholders easier. With internet access in place, it makes communications between organizations and customers very easy, it enables the organizations to work and communicate with their customers across the nation. That was emphasized by Bacal[76] when he stated that in general terms, the internet allows communication and research to be done from the office. Its valuable contribution will be in the ease that communication can occur with colleagues, and members of the public. Despite the usefulness of internet to these organizations, some of them provided access to internet with some restrictions, although some organizations provide complete internet access. Private sector organizations provided complete internet access but with some restrictions. Regulating internet comes with the organizations providing some restrictions to some sites. They block some sites that were thought could lead to low efficiency in the workplace. Such sites include pornography and online gaming sites that could distract workers. They do so by blocking some sites during the working hours and providing access by granting permission from the administrators.

Organizations also regulate internet use by monitoring employee's usage of internet or surveillance by storing and reviewing employee's computer files which a lot of organizations monitor routinely for all their employees. Sometimes this is done with the employees' knowledge, but often it is not[77]. In making the decision whether to monitor, the employer should consider the benefits and costs to both itself and its employees. According to Bezek, Britton & Curtis[78], there are several benefits to employer monitoring. First, the employer is better able to ensure that its employees are using their work hours for work. If an employee is logged into a travel web site for an hour a day, the employer will know that there is a problem. Second, the risk of the internet or e-mail being used for harassing or offensive purposes will be lessened; and if such behavior does occur, it can be corrected quickly. Thus, the employer will have a greater opportunity to provide a working environment that is not hostile or offensive or otherwise likely to lead to employee claims of harassment or discrimination. Third, monitoring may prove effective in uncovering employee misconduct, such as the unauthorized dissemination of trade secrets.

Bezek, Britton & Curtis[79] however noted that while monitoring may provide protection to an employer

because it allows the employer to remove inappropriate material, it can also end up creating liability. If an employer undertakes monitoring, he may have a higher duty to ensure that no offensive, harassing, or otherwise inappropriate material remains on the system. Also, if an employer's policy is to monitor e-mail, there is no basis for employees to have an expectation of privacy. In addition to helping create a higher duty for ensuring that the system is not used for inappropriate purposes, the lack of an expectation of privacy can create problems with employee morale[80]. Studies have shown that employees who are monitored in various ways have increased stress and fatigue, higher absenteeism, and lower morale. Perhaps it is common sense; no one feels good knowing that he is being "watched." Another potential downside for employers is that in order to create a policy that is less open to challenge, the monitoring policy should include monitoring of all employees, even at the highest levels. Management must consider whether they want their internet use and e-mail messages to be reviewed.

The survey findings showed that a lot of organizations in Botswana do not have formal policies on personal internet use in the workplace. They do not have written policies governing personal use of email, personal use of instant messaging, and personal use of internet. It showed that they still lack information on the need to implement personal internet use policies. One of the reasons might be that implementing those policies is difficult. Woodbury[81], Halbert & Inguilli[82] cited in Alampay and Hechanova[83] emphasized that doing so, however, always comes with the inherent tension between employees' rights to privacy and an organization's right for knowing and controlling what happens in the workplace. The common policies that were implemented in most of the organizations were the policy on internet use in general and the policy of monitoring email accounts. These findings are similar with those from previous studies. Finding from Alampay and Hechanova[84] study showed that new communication technologies such the internet have become more integrated into organizations and people's work in the Philippines. What appears to be lacking however, is the articulation and implementation of internet use policies. Perhaps this is the reason why Philippine organizations are encountering negative consequences including security breaches and diminished productivity. In some cases, misuse has lead to discipline and even dismissals. The same thing applies to those organizations surveyed in Botswana as the findings revealed that majority of them do not have the policies implemented to monitor the use of internet in their workplace.

According to Lease and Gordon[85] the research literature supports the authors' belief that an organization can meet the seemingly juxtaposed goals of managing employee e-mail and internet use while supporting organizational effectiveness through a clearly stated policy for the acceptable use of e-mail and internet assets. To be effective, this acceptable use policy must be crafted and administered in such a way that it clarifies the mutual expectations of both the employer and employees. It can support organizational effectiveness by:

1. Not interfering with the organization's day-to-day business operations

2. Balancing the employer's need to control e-mail and internet use with an employee's reasonable expectation of some personal use of e-mail and internet assets

3. Identifying those employees who may jeopardize the organization's effectiveness through illegal, unethical, or counter-productive activities.

Thus, for organizations considering implementing controls on employee use of e-mail and internet assets, the authors recommend that they develop a comprehensive, written policy on employee use of the internet and e-mail as well as on company programs of electronic monitoring of e-mail and internet use. This policy should communicate the rules for personal use of e-mail and internet assets – what is allowed, what is not allowed, and the rewards and penalties for following the rules. The monitoring of employee e-mail and internet use is much less of an issue when there is a clear understanding of expectations – for both the employer and the employees – and when the guidelines are relevant to the organization, its culture, and the technology it uses[86]. This type of "expectation setting" is the sort of information that might be found in an "acceptable use policy" for e-mail and internet assets. Acceptable use policies are not new; many organizations have adopted them and examples can be found readily even on the internet. As argued by Stewart[87], "often the mere existence and promulgation

of a clear policy is enough to stem most forms of internet access abuse" (p. 50). Acceptable use policies, however, do not appear to provide much support for organizational effectiveness when they are not clearly communicated and when there is a lack of integration between the policies themselves and the organization's overall strategy and vision[88].

Conclusions

This study has empirically demonstrated the practice of internet monitoring and regulation in Botswana organizations. While some organizations have policies in place to monitor, others do not. As more and more organizations are installing internet access for staff in the country, the question will be how do they regulate usage of internet in the workplace? It is recommended that the there is a need to put policies in place to have guidelines for email and internet monitoring. In essence, the creation of an effective acceptable use policy requires a comprehensive understanding of the organization's goals, internet and e-mail usage goals, specific risk profiles, and organizational culture. In developing an acceptable use policy, it is important to recognize that the "stakeholders" include all employees, third parties who might have access to organization e-mail and/or internet assets, and potentially, organized bargaining representatives (e.g., a union)[89]. Therefore, the guidelines should reflect the participation of a diverse set of employee and management representatives. Corporate communications, human resources, training, and other departments/functions that regularly communicate with employees should also be included. In addition, the Legal Department and/or an outside counsel should be consulted on obvious legal matters and may wish to advise on appropriate forms of words for the most formal awareness materials. Likewise, information security and IT experts can also provide valuable perspectives.

As with any policy, staff should be actively involved in determining what is and is not acceptable behavior on the internet. It is important to prepare an internet use policy document that advises all members of staff that their internet usage is being monitored, while setting guidelines as to what the company see as acceptable in the workplace. The policy should list acceptable use internet policies in a written document that would be circulated to all members of staff. It should also outline those practices that are unacceptable such as surfing out of personal interest during work hours; visits to explicit sites whether during work hours or not; and the downloading of unacceptable material[90]. It is important to specify the penalties that apply for breach of internet use policies and to communicate clearly the change in policy, and to make sure to give the reasons for the change.

With any policy covering areas that could be deemed as "personal" activities of employees, it makes sense to build in some level of discretion. However, to ensure that the policy is sufficiently enforceable, employers need to define clearly what does and does not constitute acceptable behavior with regard to e-mail and internet use. This is to avoid conflicts or tension between the management and the employees that those policies might violate their rights as workers. Written policies, formal training, and proper management can also help minimize risk and maximize compliance to organizational and legal regulations. As such, educating Botswana organizations and their employees regarding the development of rational internet use policies is as important as the technological solutions already available. Hence, as internet use policies in organizations increasingly become a norm among organizations, this may lead employees to be less critical about the issues associated with the practice[91].

Acknowledgements

The authors thank Erwin A. Alampay and Ma. Regina M. Hechanova of University of the Philippines and Ateneo de Manila University respectively for granting the permission to use an adapted version of their survey instrument to carry out the study.

References

1. Cole J, Surveying the digital future: Year four. Ten years, Ten trends, Los Angeles, CA: USC Annenberg School Center for the Digital Future (2004). Available at: http://www.digitalcenter.org/downloads/DigitalFutureReport-Year4-2004.pdf. (Accessed on 17 February 2010).
2. Anandarajan M, Teo T S H and Simmers C A, The internet and workplace transformation. M.E.Sharpe, Inc. USA (2006) p 12-23.
3. Bacal R, Abuse of internet Access at Work. (1996) p 1-12. Retrieved: February 17, 2010, from http://work911.com/articles/inabuse.htm.
4. TechGenix Ltd. Internet Access Control. (2010) Retrieved February 17, 2010. Form http://www.isaserver.org/articles/Internet_Access_Control303.html

5. Op cit Anandarajan et al.
6. Deibert R, Palfrey J, Rohozinski R and Zittrain J, (Eds) *Access Denied: The Practice and Policy of Global Internet Filtering*, The MIT Press (2008).
7. Alampay E A and Hechanova M R, Monitoring Employee use of the Internet in Philippine Organizations, *The Electronic Journal on Information Systems in Developing Countries*, 40(5) (2010) 1-20. Retrieved February 02, 2010, from http://www.ejisdc.org.
8. Whitty M T, Surveillance & Society. (2004) Retrieved February 28, 2010 from http://www.surveillance-and-society.org/articles2(1)/filtering.pdf
9. Bonsor K, Is your workplace tracking your computer activities? (1998) Retrieved June 2010, from http://computer.howstuffworks.com/workplace-surveillance.htm/printable.
10. Bacal, *Op. Cit.*
11. Anandarajan et al., *Op. Cit.*
12. Zuckerman E, 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, (2010) p. 71-85.
13. Alampay and Hechanova, *Op. Cit.*
14. Bacal, *Op. Cit.*
15. Anandarajan et al. , *Op. Cit.*
16. Newhagen J E and Rafaeli S, Why communication researchers should study the Internet: A dialogue, *Journal of Communication*, 46 (1) (1996) 4-13.
17. Anandarajan et al. , *Op. Cit.*
18. Ibid
19. Bacal, *Op. Cit.*
20. Bonsor, *Op. Cit.*
21. Whitty, *Op. Cit.*
22. Lease D R and Gordon J, Balancing Productivity and Privacy: Electronic Monitoring of Employees (2005) Retrieved February 28, 2010 from http://www.drdavidlease.com/user/Employee%20Monitoring.pdf
23. Ciocchetti C A, Monitoring Employee E-mail: Efficient Workplaces Vs. Employee Privacy. Duke Law and Technology Review, Vol. 26, (2001) 1-12. Retrieved June 16, 2011 from http://www.law.duke.edu/journals/dltr/articles/2001/dltr0026.html
24. Lease and Gordon, *Op. Cit.*
25. Towns D M and Johnson M S, Sexual harassment in the 21st century: E-harassment in the workplace, *Employee Relations Law Journal*, 29 (1) (2003) 7-25.
26. American Management Association (2001, April). 2001 AMA survey on workplace monitoring & surveillance: summary of key findings. AMA Research. Retrieved November 3, 2004 from: http://www.amanet.org/research/pdfs/emsfu_short.pdf
27. Towns and Johnson, *Op. Cit.*
28. Lease and Gordon, *Op. Cit.*
29. American Management Association (2004, July 12). 2004 survey on workplace e-mail and IM reveals unmanaged risks. AMA Press release. Retrieved November 3, 2004 from http://www.amanet.org/books/catalog/0814472532_survey.htm
30. Maher K, Career Journal: Big employer is watching: Companies monitor workers with high tech systems; did lunch take too long? *Wall Street Journal,* (2003) p. B1.
31. Canoni J D, Location awareness technology and employee privacy rights, *Employee Relations Law Journal*, 30 (1) (2004) 26-31.
32. Forelle C, On the road again, but now the boss is sitting beside you; workers chafe as business embraces GPS trackers. *Wall Street Journal*, (2004) p. A1.
33. Lane F S, *The naked employee: How technology is compromising workplace privacy*. New York: Amacom (American Management Association). (2003)
34. Forelle, *Op. Cit.*
35. Lane, *Op. Cit.*
36. Lease and Gordon, *Op. Cit.*
37. Ibid
38. Nolan D R, Privacy and profitability in the technological workplace, *Journal of Labor Research*, 24 (2), (2003) 207-233.
39. Hubbartt W S, *The new battle over workplace privacy: Safe practices to minimize conflict, confusion, and litigation.* New York: Amacom (1998) (American Management Association).
40. Stone D L and Stone-Romero E F, A multiple stakeholder model of privacy in organizations. In M. Schminke (Ed.), *Managerial ethics: Moral management of people and processes*. Mahwah, NJ: Lawrence Erlbaum Associates, Publishers (1998) p 35-60.
41. Martin K and Freeman R E, Some problems with employee monitoring, *Journal of Business Ethics*, 43 (4) (2003) 353-361.
42. Frayer C E, Employee privacy and Internet monitoring: Balancing workers' rights and dignity with legitimate management interests, *Business Lawyer*, 57 (2) (2002) 857-876.
43. Lane, *Op. Cit.*
44. Ambrose M L, Alder G S and Noel T W, Electronic performing monitoring: A consideration of rights. In M. Schminke (Ed.), *Managerial ethics: Moral management of people and processes*. Mahwah, NJ: Lawrence Erlbaum Associates, Publishers (1998) p 61-80.
45. Lane, *Op. Cit.*
46. Hovorka-Mead A D, Ross W H, Whipple T and Renchin M B, Watching the detectives: Seasonal student employee reactions to electronic monitoring with and without notice, *Personnel Psychology*, 55 (2) (2002) 329-363.
47. Moorman R H and Wells D L, Can electronic performance monitoring be fair? Exploring relationships among monitoring characteristics, perceived fairness, and job performance, *Journal of Leadership & Organizational Studies*, 10 (2) (2003) 2-16.
48. Zweig D and Webster J, Where is the line between benign and invasive? An examination of psychological barriers to the acceptance of awareness monitoring systems, *Journal of Organizational Behavior*, 23 (2003) 605-633.

49. Ambrose et al, *Op. Cit.*
50. Lane, *Op. Cit.*
51. Stanton J M, Traditional and electronic monitoring from an organizational justice perspective, *Journal of Business & Psychology*, 15(1) (2000) 129-147.
52. Hubbartt, *Op. Cit.*
53. Lease and Gordon, *Op. Cit.*
54. Nolan, *Op. Cit.*
55. Lease and Gordon, *Op. Cit.*
56. Nolan, *Op. Cit.*
57. Martin and Freeman, *Op. Cit.*
58. Alge B J, Ballinger G A and Green S G, Remote control: Predictors of electronic monitoring intensity and secrecy, *Personnel Psychology*, 57(2) (2004) 377-410.
59. Lane, *Op. Cit.*
60. Lease and Gordon, *Op. Cit.*
61. Stanton, *Op. Cit.*
62. Vaught B C, Taylor R E and Vaught S F, The attitudes of managers regarding the electronic monitoring of employee behavior: Procedural and ethical considerations, *American Business Review,* 18(1) (2000) 107-114.
63. Zweig and Webster, *Op. Cit.*
64. Moorman and Wells, *Op. Cit.*
65. Hovorka-Mead et al, *Op. Cit.*
66. Cialdini R B, Petrova P K and Goldstein N J, The hidden costs of organizational dishonesty: Companies that engage in unethical practices face consequences far more harmful than is traditionally recognized, *MIT Sloan Management Review*, 45(3) (2004) 67-74.
67. Alge et al, *Op. Cit.*
68. Ambrose et al, *Op. Cit.*
69. Lane, *Op. Cit.*
70. Hubbartt, *Op. Cit.*
71. Ambrose et al, *Op. Cit.*
72. Lease and Gordon, *Op. Cit.*
73. Ambrose et al, *Op. Cit.*
74. Lane, *Op. Cit.*
75. Stanton, *Op. Cit.*
76. Bacal, *Op. Cit.*
77. Bezek P J, Britton S M and Curtis R A, Employer monitoring of employee internet use and email: nightmare or necessity? *MEALEY'S Cyber Tech Litigation Report*, 2(11) (2001) 1-8.
78. Ibid
79. Ibid
80. Ibid
81. Woodbury M, *Email, Voicemail, and Privacy: What Policy is Ethical?*, The Fourth International Conference on Ethical Issues of Information Technology, Erasmus University, The Netherlands, 25-27 March (2008). http://cpsr.org/prevsite/~marsha-w/emailpol.html.
82. Halbert T and Inguilli E, *Cyberethics*, Cincinnati: West Thomson Learning (2002).
83. Alampay and Hechanova, *Op. Cit.*
84. Ibid
85. Lease and Gordon, *Op. Cit.*
86. Ibid
87. Stewart F, Internet acceptable use policies: Navigating the management, legal, and technical issues, *Information Systems Security,* 9(3) (2000) 46-52.
88. Lease and Gordon , *Op. Cit.*
89. Ibid
90. Bonsor, *Op. Cit.*
91. Alampay and Hechanova, *Op. Cit.*