European Journal of Business and Management
ISSN 2222-1905 (Paper) ISSN 2222-2839 (Online)
Vol.7, No.9, 2015


# Information Technology Innovation and Organizational Policy: Implications on Employee Privacy

Bengat K. Joseph[1]
Department of Business Management Studies, Kenya Highlands Evangelical University, Kericho, Kenya
Email: kipyegonarapbengat@yahoo.com

Dr Tubey R. J [2]
Department of Entrepreneurship Studies, School of Human Resource and Development Studies
Moi University, Eldoret
Email: ruthtubey@gmail.com

Jacob K. Rotich[3]
Department of Development Studies, School of Human Resource Development,
Moi University, Eldoret, Kenya
Email:richardorich@gmail.com

**Abstract**
Issues relating to workplace privacy and how organizations address privacy have sparked a lot of public debate in recent years. Research reveals that potential employers have exploited employees seeking job opportunities by asking information to do with: disclosure of confidential information about the past employer's work, financial background, and family intimate issues not relevant to the job being sought among others. This paper establishes the implications of information technology innovation on organization policies with emphasis on employees' privacy. The study was done in two organizations and it adapted a case study approach. Data was collected from 74 respondents using questionnaires. Respondents were sampled using purposive technique. Frequency distribution tables were used in data presentation followed by discussions. The findings of this study are critical in informing the policy makers in organizations on procedures and strategies of inclusive policy formulation and implementation as well as provide HR managers with insight on managing privacy issues in dynamic organizational setups.
**Key words**: Employees' Privacy policy, Information Technology, Surveillance

## Introduction

HR professionals are often at the forefront of developing policies concerning the use of social media whether by the organization or employees themselves. A 2012 survey revealed that 40% of organization have social media policies and from that groups 43% of organization said the HR department is primary responsible for creating social media policies. Another 44% said that HR is also in charge of enforcing those policies (SHRM, 2012). Enhancements of IT operations are an integral part of many HR professionals business plans. Technological changes in the work place have been extremely fast paced over the past decade with the emergence and use of fiber optics. New technology and software have streamlined HR processes and made it easier to access and use valuable data within and outside the physical precincts of the organization. The new trend in the work place is the use of mobile phones which has literally penetrated almost all operations of organizations. With these dynamic changes, organizations have not only embraced the use of mobile phones as a tool of communication but have also recognized that mobile devices are crucial to their own success, and many have incurred significant expenses purchasing and securing such devices, and equipping their workforce. Employees are increasingly using (or demanding to use) personal devices to store and process their employer's data, and connect to their networks.

Findings show that at the start of 2008; there were only three million apple iPhone mobile devices in the world (Global Human Capital Trends, 2014). At the end of 2013 according to Gartner estimates, there were 1 billion smart phones and more than 420 million iPhones mobile devices shipped (Gartner Estimates 2014). Facebook had a million users in 2004, 100 million in 2008, and estimated 1.23 billion registered users by 2014. Today employees are online 24/7 and are relentlessly flooded with information, messages and communications. The benefits enjoyed by technological advancement in the workplace have come with risks. As such, increased vigilance against cyber-attacks and enhancement to it operations are an integral part of many HR professional's business plans.

A research on 'the top workplace trends' according to HR professional (SHRM, 2013) covering a period of 2003 to 2011 showed that the first in 2003 was use of a technology to communicate with employees with the third being increased vulnerability of intellectual property and the tenth being ability to use technology to move closely to monitor employees.

The same research showed that in 2005 there was a growing complexity of legal compliance which was trending at position four while at position five was use of technology to perform transactional HR functions.

 

In 2007 vulnerability of technology to attack disasters trended at position ten and by 2011 growing complexity of legal compliance for employees and changes in employees' rights due to
Legislature or court rally trended at position four and five respectively. In all this, technology as a means of communication is taking center stage of any business operations. The same research contends that about 65% of the C.E.Os argued that they were addressing these challenges by updating technology use policies for employees (which covered use of social networking sites and mail for non-business e.t.c) while 54% argued that they were changing employment practices to minimize legal risk. With increase of mobile communications comes in the growth of social media. Social media websites have become a popular platform that many Kenyan organizations use to build new relationships and content. However, social media websites are also being used by cyber criminals to indulge in various cyber- crimes. In 2013, the number of criminal offences related to social media websites in Kenya increased (Kenya Cyber Security Report 2014). During the west-gate attack (21st September 2013), the terrorists utilized social media such as twitter to gain information on the efforts being conducted by the police. The occurrence of such magnitude raises concerns in management whether to monitor every conversation that takes place in organization premise or not. The leaking of information through digital means is often considered an 'insider' job. Clearly insider jobs remained the biggest problems in organizations in 2013. Privileged users propped systems for a variety of reasons including disgruntlement, revenge, competitive advantage and blackmail. The scope of insider job threats intensified as business models continued to evolve with increased mobility, growing mix of users and geographically diverse business offices (Kenya Cyber Security Report 2014)

These arguments boils to one thing: technology is not only critical but it also comes with its challenges. The overriding question, however, is: Are HR professionals well versed with formulation of IT systems security policies that safeguard on employees' privacy? , How will these be possible without infringing into one's privacy rights? Are the polices wide enough to match the dynamic technological innovations more so in mobile gadgets?

**Literature Review**

**Employees' privacy**

Kenya's new constitution (ROK, 2010) provides privacy as a human right under article 31(a to d) which states that "Every person has the right to privacy, which includes the right not to have: their person, home or property searched, their possession seized, information relating to their family or private affairs unnecessarily required or revealed; or the privacy of their communications infringed' Employees' privacy at workplace is an issue that has raised debate worldwide (Sandeep K Krishnan, Biju Varkkey & Anush Raghavan, 2006). Employee privacy can be defined as 'Freedom for employees from unauthorized intrusion from employers' (Bennett & Locke 1998). Research reveals that potential employers have exploited employees seeking job opportunities by asking information to do with: disclosure of confidential information about the past employer's work, financial background, and family intimate issues not relevant to the job being sort among others (Sandeep et al, 2006). The emerging technological innovation has tremendously increased the way information is handled in workplace.
The 2005 American Management Association and the policy Institute survey showed that nearly three-fought of the companies admitted to have been exercising some of electronic surveillance over their employees (AMA, 2005). The same survey done in 2007 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. The report showed that employers are concerned about employees visiting adult sites with sexual content, as well as games, social networking, entertainment, shopping and auctions, sports, and external blogs. Of the 43% 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. A leading telecommunications service provider sacked 33 employees over cases of economic crime, including accounting fraud and asset misappropriation. A leading commercial bank employee was charged with defrauding the bank of Sh60 million (Kenya Cyber Security Report 2014)

Over ninety percent of private sector persons no longer enjoy the privacy protectors afforded by collective bargaining relations, under common law doctrines, they constitute "at will" employee who can be terminated by their employers at any time for good cause, bad cause, or no cause (Mark A.Rothstein et al, 2004)

With technological innovations work place has now seen smartphones, tablets, laptops, netbooks, desktops, amongst the device options individuals have these days (and within each category additional brand [iPhone v. Android], software and operating system choices exist). At the same time, organizations have recognized that mobile devices are crucial to their own success, and many have incurred significant expense purchasing and securing such devices, and equipping their workforce. Nonetheless, employees are increasingly using (or demanding to use) personal devices to store and process their employer's data, and connect to their networks. These and many more illustrate how permeable society is when it comes to information

 

flow. If HR Managers will not be proactive in managing these information and means by which the same information is passed, then organizations are likely to stock a 'disaster in waiting' Thus, most management members of organizations are at a cross roads with regard to establishing strict policy framework, which may violate human rights, or operating in a laize-faire at the detriment organizational most crucial information. The reasons for this vary from avoiding the need to carry and manage multiple devices, to the desire to use the most up-to-date devices that exist, to increased efficiency.

Inevitably, technology will be able to breach all possible individual privacy without the person actually being able to understand the situation (Sandeep et al, 2006). Such monitoring is virtually unregulated. Therefore, unless company policy specifically states otherwise (and even this is not assured), your employer may listen, watch and read most of your workplace communications. With technological innovations, organizations need to: Maintain the security and confidentiality of client records, protect against internal and external threats to the security or integrity of such records, protect against unauthorized access or use of client records or information that could result in substantial harm or inconvenience to the client.

**Organization scenarios**

There has been attempt in work place to censor information flow from employees. For instance, businesses sites privacy interest to limit employees discussion of issues that do not directly involve organizational activities ,e.g. many organization prohibit workers from sharing information pertaining to compensation levels and they discipline employees who discuss such "confidential" information, (Charles Op Cit -2006).

Privacy-related concerns arise regularly in employment setting. Employers assert private property rights to restrict the organization activities of both employees and non-employee union organizers (Charles B.Craver, 2006)

Charles argues that such organizations assert privacy claims when representative labor organization request access to confidential company financial records or similar privileged information. He further contends that employees frequently discount employee privacy claims when they monitor worker activities through closed-circuit television cameras and access to employee email exchange s and internet activities. Charles (op at) posits that firm ignores worker privacy interest when they conduct expensive pre-employment medical examination and administer tests that purport to measure applicant honesty and other personality traits.

Charles (2006) explores employer restrictions on other forms of employee communication. He argues that business is privy concern to limit other forms of employee emerging communication. Such business frequently tries to prevent workers from exchanging organization message with coworker or outside organizers via e-mail system or through internet sites. The argument of such institution is that these restrictions are necessary to preserve the privacy of employer-provided corrupters (United service Automobile Association 2003). The irony for this is , whereas organizations and "micro manage' the use of computers the same information can be passed through smart phones, which in most cases are individually owned and which organizations may not be able to control. Employee's may be sending confidential, sensitive or offensive information across a corporate network with the sincere belief that their communications are private (Wakefield 2014).However-mail can be easily distributed ,copied and read by numerous others without the sender's knowledge. E-mail distributed within networks is stored on the system even through receivers and senders may have deleted the message.

Research shows that business appreciates the fact that supervisors cannot partially monitor the activities of their workers at all times and they often use electronic devices to facilitate this process, many companies have installed closed circuit television cameras to enable awareness to observe different areas simultaneously. These may cover work areas and work areas that are open to public scrutiny such as a general production and service spaces, corridors and parking. Charles (2006) argues that since employees do not have any reasonable expectation of privacy while they are working or walking in these public areas, these monitoring activities do not contravene their basic rights.

The critical issue then is when does privacy infringement occur? Charles contends that when such cameras are surreptitiously placed in areas like worker rooms or laboratories without employees' notification are courts in key find impermissible invasion of individual privacy interest. Timkin (2002) pointed out that if cameras or microphones are used to spy upon the protected organizational activities of employees during their non-work time, unfair practice liability is likely to attach. The argument here is if such digital devices are used as with employee's awareness that their actions are being observed, then privacy issue is not violated. Thus when firms use cameras to monitor open areas of their facilities, they should notify workers of the fact they are subject to electronic observation. Although most people believe that employers do not have the right to monitor worker phone calls, many companies monitor telephone calls made by employees or use hidden microphones to listen to oral conversation involve their worker most states have laws restricting the secret monitoring of telephone and oral communications (Roltstein et al 2004). In order not to create frictions with employees, organizations ought to rethink how this can be done without prejudicing against one party.

 

**IT innovation and Privacy policies**

In the last 20 years, new communication technology, such as email, mobile phones and web and videoconferencing has not only facilitated closer contact with clients in distant lands, it has allowed multinational companies to form cross-border teams, where colleagues can communicate with each other constantly, despite not being located in the same place. In short, technology has enabled the international expansion that companies seek. (SHRM, 2006)

Technological changes in the work place have been extremely fast paced over the past decade.

New technology and software have streamed lined HR processes and made it easier to access and use valuable data. Technological advancement has made it possible to conduct business virtually anywhere in the world. More organizations are taking advantage of the ability to expand their brand so as to connect their workforces (SHRM, 2012, July) Such advances have revolutionized most industries, transforming nature of the task of most employees, the type of activities they engage in and their responsibilities (The Economics Intelligence United Ltd 2014). By widening the scope and mode of operations, technology has reconfigured HR tasks and responsibilities. An increased reliance on high-technology has also necessitated greater investment in cyber security.

New skills measures in the workplace and HR professionals are on guard against internet fraud, identity theft and other tech-based criminal actions. Therefore, though technology has made numerous aspects of business operations much more efficient, rapid technology advancement have sometimes made it difficult for business and individuals to keep up (SHRM, 2012).The benefits enjoyed by technological advancement in the workplace have come with risks increased vigilance against cyber-attacks and enhancement to it operations are an integral part of many HR professional's business plans.

A research on 'the top workplace trends' according to HR professional (SHRM,2013) covering a period of 2003 to 2011 showed the first in 2003 was use of a technology along to communicate with employees with the third being increased vulnerably of intellectual property and the tenth being ability to use technology to move closely to monitor employees. The same research showed that in 2005 there was a growing complexity of legal compliance which was trending at position four while at position five was use of technology to perform transactional HR functions.

In 2007 vulnerability of technology to attack disasters trended at position ten and by 2011 growing complexity of legal compliance for employees and changes in employees' rights due to legislature or court rally trended at position four and five respectively.

In all these, technology as a means of communication is taking center stage of any business operations. In a research done, about 65% of the C.E.O.s argued that they are addressing these challenges by updating technology use policies for employees (which covered use of social networking sites-mail for non-business e.t.c) while 54% argued that they are changing employment practices to minimize legal risk. These arguments boils to one thing: technology is not only critical but it also comes with its challenges. This implies that spending on IT security will remain a priority for the organization. According to technology research firm Gatner Inc; IT security spending was expected to reach 60 billion worldwide, in 2012 up 8.4% from 2011 and by 2016, it is expected to reach 86 billion. This report asserts that this can be reduced if effective policies are put in place and efficiency implemented. It is shown that even with security measures in place hackers and other criminals are still finding ways to steal and wreak havoc on computers systems. A combined 88% of respondents said the loss of employees' privacy as a result of technology has an impact in workplace. Even when we don't intentionally provide personal information online; that information is being tracked and often shared without employees know ledged.

A wall street journal survey of 50 websites found that 12 of those sites sent potentially identifying information, such as criminals' addresses or full real names to third parties. Another segment of the wall streets journal's examination focused on 1000 websites with researchers finding that 75% of the sites now include code from social networks such as Facebook and twitter. This code can match people's identities with their web checked. (Valentinon device; & Singer-vine2012)

**HR Managers' dilemmas**

While managers may have a right to monitor regularly employees to be sure they are performing their assigned job task and are not engaging in impermissible conduct during their work time. They may not have a right to engaged in surveillance of protected concerted activities during the non-work time of employees, monitoring their employees will be unfair labor practice liability (Scot Cox et al, 2005). The greater monetary risk to employers from access to email and internet activities by employees would involve claims of tortious privacy invasion.

Most courts have held that workers do not have a reasonable expectation of privacy when they use computers provided by their employees. Telephone, email, and internet monitoring present more complex privacy issues, on the other hand, firms want to be sure employees are performing their assigned job task during work hours and they wish to preclude worker use of these media for improper purpose such as the harassment of coworkers, access to pornographic sites or the discourse of confidential corporate information. On the other hand, workers who are permitted to use these communication channels for

 

personal reasons have the right to expect their appropriate exchange with coworkers and outside persons will remain confidential. How companies can simultaneously honors this seemingly contradictory phenomenon without infringing on employees' privacy is a big dilemma. It is imperative that proper policy formulation should be put in place which is the purview of the HR. Proactive measures should be put in place to address this dilemma. For instance, companies should initially notify employees that their phone calls, e-mail exchange and internet activities are subject. Robin (op cit) points out that electronic monitoring is reasonable when there is a business purpose, policy exist to set the privacy expectations of employees, and employees are informed of organizational rules regarding networks activities and understand the means used to the workplace.

Thus, organization should obtain consent from employees regarding monitoring or surveillance activities. Organizations are legally liable for all communications originally from their networks regarding all policy issues more so if violation of such policy (ies) has occurred.

**Methodology**

This study opted to use case study approach focusing organization to come up with reliable and credible information that informed this research

**Findings**

Data was collected from 74 respondents 53 of whom were male (71.6%) and 21 female (28.4%) employees. These respondents were randomly sampled from departments considered to be mostly involved with communication. These are: HR and Employee welfare, Marketing, Customer care and Public Relations office and Administration.

**2.4.1 Distribution of Employees according to Gender**

| Gender | Frequency | Percent |
|---|---|---|
| Male | 53 | 71.6 |
| Female | 21 | 28.4 |
| | 74 | 100.0 |

**Source: Author's research data (2015)**

The first task was to examine if privacy policies exist in the organization under study.

**Table 2.4.2: Privacy policy exists**

| Response | Frequency | Percent |
|---|---|---|
| Yes | 3 | 4.1 |
| No | 71 | 95.9 |
| **Total** | **74** | **100.0** |

**Source: Author's research data (2015)**

Table 2.4.2 shows the existence of privacy policy in the organization understudy. The findings of this research revealed that 95.9% of the respondents pointed out that privacy policy in their institution do not exist while only 4.1% argued that the policy existed where they work. Where the policy exists, it was revealed that most employees were not aware of the contents of privacy policy with total respondents of 82.4% affirming this view (18.9% Disagreed and 63.5% strongly disagree) as shown in table 2.4.3. This implies that violating their rights with regard to privacy issues is easy because unless one is aware of his /she rights it becomes a big challenge not only to identify instances of violation, but also how to address the legality of it.

 

**Table 2.4.3: Policy contents are known by all employees**

| Response | Frequency | Percent |
|---|---|---|
| SA | 3 | 4.1 |
| A | 8 | 10.8 |
| UD | 2 | 2.7 |
| D | 14 | 18.9 |
| SD | 47 | 63.5 |
| **Total** | **74** | **100.0** |

**Source: Author's research data (2015)**

An analysis of employees' response showed that most of the employees (86.5%) observed that ICT has greatly influenced communication in the organization (Table 2.4.4). It was clear that mobiles, computerized systems and its applications play a significant role in daily operations. Computer systems with its applications was said to be prone to abuse and was also easy to monitor its usage.

**2.4.4: ICT has greatly influenced communication in the organization**

| Response | Frequency | Percent |
|---|---|---|
| SA | 41 | 55.4 |
| A | 23 | 31.1 |
| UD | 8 | 10.8 |
| D | 2 | 2.7 |
| SD | 0 | 0.0 |
| **Total** | **74** | |

**Source: Author's research data (2015)**

Employees observed that it was easy to detect spying or intrusion when one is using computer than when one is using a mobile phone. Email hacking was noted to be common in organization and this alerted most employees that their privacy when using such gadgets in workplace was not guaranteed. Table 2.4.5 shows employees' perception on violation of violation of privacy policy.

**Table 2.4.5: There is constant violation of the policy by top management**

| Response | Frequency | Percent |
|---|---|---|
| SA | 42 | 56.8 |
| A | 26 | 35.1 |
| UD | 4 | 5.4 |
| D | 2 | 2.7 |
| SD | 0 | 100.0 |
| **Total** | **74** | |

**Source: Author's research data (2015)**

 

The findings showed that 91.9 % of employees confirmed the view that most organizations have violated employees' privacy (AMA, 2005).

Additionally, the study revealed that the organizations under study utilized social media, Emails and written communication was a common mode of communication among employees. Social media was prominent among these modes scoring 62.1% of the total respondents followed by use of emails (28.4%) and written mode (9.5%). It was however noted that where written mode was used the communication tended to be official as in case of internal memos and notices. The emails were mainly used for convening meetings and circulating important policies and reports as well as passing policy matters. Table 2.4.6 gives a summary of common means of used by employees among themselves.

**Table 2.4.6: Most common means of communication between employees**

| Response | Frequency | Percent |
|---|---|---|
| Social media | 46 | 62.1 |
| Email | 21 | 28.4 |
| Written | 7 | 9.5 |
| **Total** | **74** | **100.0** |

**Source: Author's research data (2015)**

An attempt was also made in this study to examine the common means of communication utilized by organizations under study. Table 2.4.7 reveals that Mobile call and SMS was mostly used to reach out to employees (43.2%), Email (33.8%) and internal memos (23.0%). Clearly, it can be seen that organizations are shifting from traditional modes of communication like Memos, notices and announcements to embrace new and modern technological approaches like mobiles. Thus organizations are becoming more and more vulnerable to intrusion if strategies of ensuring security in passing information are not put into place.

**Table 2.4.7: How organizations communicate with employees**

| Response | Frequency | Percent |
|---|---|---|
| Email | 25 | 33.8 |
| Mobile call and SMS | 32 | 43.2 |
| Internal Memos | 17 | 23.0 |
| **Total** | **74** | **100.0** |

**Source: Author's research data (2015)**

This study found that despite the increased in sophistications in mode of communications used in organizations, most employees felt that privacy was not guaranteed. A greater number of respondents (91.9%) cast aspersion on privacy in using identified media with only 8.1% expressing confidence in the use of these media. This is shown on table 2.4.8. Thus, there is an increasing believe among employees that their communication in whichever media is being infiltrated by external unwelcomed character

 

**Table 2.4.8: Privacy through identified media is assured**

| Response | Frequency | Percent |
|---|---|---|
| Yes | 68 | 91.9 |
| N o | 6 | 8.1 |
| **Total** | **74** | **100.0** |

**Source: Author's research data (2015)**

As a result of insecure environment most employees opined that they did not enjoy communicating freely without fear of being spied on with 87.8% (39.2% Disagreed and 48.6% strongly disagreed). The implication of this is that most organizations are overwhelmed by state of insecurity in their private issues from technological innovations that originally was meant to enhance communication (Table 2.4.9)

**Table 2.4.9: Employees enjoy freedom of communication without fear of being spied on**

| Response | Frequency | Percent |
|---|---|---|
| SA | 2 | 2.7 |
| A | 3 | 4.1 |
| UD | 4 | 5.4 |
| D | 29 | 39.2 |
| SD | 36 | 48.6 |
| **Total** | **74** | **100.0** |

**Source: Author's research data (2015)**

The argument being put forward by most respondents is that technology, and mainly emergence of mobile communication, has negatively impacted on privacy when it comes to communication.

**Table 2.5: Emergence of mobile communication has negatively impacted on privacy**

| Response | Frequency | Percent |
|---|---|---|
| SA | 46 | 62.2 |
| A | 12 | 16.2 |
| UD | 9 | 12.2 |
| D | 3 | 4.0 |
| SD | 4 | 5.4 |
| **Total** | **74** | **100.0** |

**Source: Author's research data (2015)**

Table 2.5 show 62.2% of respondents and 16.2% (78.4%) pointed that emergence of communication has negatively impacted on privacy. This is not only because of the fact that those involved in communication fear being spied on but because they are at times tempted to spy on others in social media. Table 2.5.1 shows respondents' views on social media. A largest number of respondents (91.9%) are of the opinion that social media has negatively impacted on communication (60.8%, Strongly Agree and 31.1% Agree). Most written communication observes grammatical rules, tenses and phrases which can be contextualized and meaning deciphered. However social media has seen varied emergence of new language which only members of that social group can understand.

 

**2.5.1: Social media platform has impacted negatively on communication**

| Response | Frequency | Percent |
|---|---|---|
| SA | 45 | 60.8 |
| A | 23 | 31.1 |
| UD | 4 | 5.4 |
| D | 2 | 2.7 |
| SD | 0 | 0.00 |
| **Total** | **74** | **100.00** |

**Source: Author's research data (2015)**

**Discussions and conclusions**

This study sought to find out the implications of Information Technology Innovation on Organization Policies with emphasis on Employees' Privacy Policies in Work place.

While most organizations have been able to safeguard against cybercrime in their computer systems through surveillance and other strategies(which violates right to privacy) Organizations are yet to craft strategies of ensuring ethical use of Mobile phones in their work place without over stepping its mandate and infringing in employees' privacy. This is in spite of the fact that mobile phone industry is astronomically growing and is slowly 'replacing' computers and desk top. From the preceding discussion technological innovation and digital convergence in the world has revolutionized knowledge, change society and operations in work place. Technology has raised complex ethical, legal and several issues. People are faced with complex and difficult question regarding the freedom of expression, access to information, the right to privacy, intellectual property rights and cultural diversity. Violation of these rights have created new problems in human social media, such as the digital divide, cybercrime, digital security and privacy concerns all of which have affected people's relations in workplace. Human rights in terms of freedom of expression and the protection of confidentiality of personal data is under threats as organizations grapple with the need to secure its information, protect is credibility and respect the human right of privacy. Thus, as organization embrace technological changes; they should factor in legal implications that may endanger its operations should they be found to violate employees' privacy. Security has been shown to be a fundamental principle of any democratic society in the I.C.T world and synergy between ICT policy and Employees' privacy policy should be established to safeguard both the interests of the organization and employees.

The scenario is even more complicated by the emergence of human security threats perpetuated by radical groups like Al-shabaab in Kenya and Somalia, and Boko Haraam in Nigerial among other radical groups. While the governments are committed to safeguard against threats of its people, organizations are called upon to put security measures in their work place. It may imply that such organizations may be forced to monitor the calls of its clients as well as those of its employees. This is another dilemma which managers will face, they can convince their employees that are worth to monitor communication but how will the clients take it?

Any failure to effectively communicate the rationale of such policy to all stakeholders is likely to bring operations at a halt.

One clear impediment of any policy implementation is failure to communicate during its formulation stage. If the policy formulation is all inclusive, employees would be highly involved and create awareness among new employees joining the organization. If sensitization and dissemination of such policy is made available to clients, they will be able to understand and operate in such environments. When an employer states a policy regarding any issues in the workplace which may include privacy issue, that policy is legally binding to all members of the organization irrespective of their ranks.

Policies can be communicated in various ways: through employee handbook, via memos, and in union contracts for example, if an employer explicitly states that employees will be notified when telephone monitory takes place, the employer generally must honor that policy. Balancing monitoring and employees' privacy is achievable with minimal stress when organizations has informed employees of the purpose of monitoring activities, set privacy expectations and create reasonable monitoring policies. The preceding discussion has also pointed out that in their attempt to monitor employees privacy, there is always an excuse that managers realize the need to protect the organization from employees activities over firm networks outweigh employees claims for privacy in the workplace. He argues that surveillance of cooperate networks can moderate the temptations to use employer resources for personal use and encourage employees to adhere to company's policies. Reducing the vulnerabilities posed by internal users' needs to be a key priority in Kenyan organizations' security strategies. Kenyan organizations need to look at holistic solutions which include controlling access rights, reviewing activity, analyzing

 

anomalous behaviors, monitoring inbound and outbound traffic for confidentiality violations, and encrypting data (Kenya Cyber Security Report 2014)

**Recommendations**

It has come out from this research that most organizations have no written policy on privacy and how to safeguard such privacy of its employees. It is on the basis of this that it is recommended that organizations have written policy clearly stating that right to privacy the point at which privacy is said to have been violated and procedure of addressing such a violation. It is also recommended that organizations develop policies governing the use of mobile phones in work with regard to workplace related issues to be communicated via mobile phones.

Despite the fact that there is critical challenge in implementing privacy policy in the wake of new technology, balancing the legitimate need of the employers to monitor the workplace with respect for individual privacy is not difficult. The best cause of action should be to develop monitoring policy which stipulate when monitoring is done and how issues private can be isolated with those that are detrimental to organizations' operations.

Where privacy policy exists it is covert and some employees do not know. Organizations should sensitize all the stakeholders on existence of such policy and the grounds at which implementation can be done.

Ethical issues should be explicitly indicated in the policies governing use of communication gadgets in workplace. In doing so the stakeholders are likely to evade issues of litigation.

**References**

Adams, Hall; Suzanne M. Scheuing; Stacey A. Feeley; 2000)

AMA (2001) Workplace Monitoring and Surveillance Report, American Management Association.

Bennett,S.C. & Locke, S.D (1998) Privacy in the Workplace: A Practical Primer . Labour Law Journal, 49(1): 781-788

Charles B. Craver (2006) Privacy Issues Affecting Employers, Employees, and Labor Organizations. GW Law Faculty Publications and Other Works

Gartner estimates, January 7, 2014 http://www.gartner.com/newdom/id/2645115.

Global Human Capital Trend (2014).Engaging the 21st Century Workforce Apple Inc

IMPAC (2010) International function of Research in applied Natural and social sciences (htt:/impact.bersin.com)

Kenya Cyber Security Report 2014: Rethinking Cyber Security- "An Integrated Approach: Processes, Intelligence and Monitoring" TESPOK

Mark A. Rothstein, Charles B. Craver, Elinor P. Schroeder & Elaine W. Shoben (2004) Employment Law Treatise

Robin L. Wakefield (2014) Employee Monitoring and Surveillance-The Growing Trend. CPA Journal, Information Systems Control Journal

ROK (2010) The Proposed Constitution of Kenya 6th May. Government Printer; Nairobi

Sandeep K Krishnan, Biju Varky & Anush Raghavan (2006) Employee Privacy at Workplaces: Some Pertinent Issues. Indian Institute of Management Ahmedabad-380015 W.P.2006-02-04

Society for Human Resource Management (2012, August) From e-learning to Mobile Learning: HR management. Retrieved from: http://www.shrm.org/publication/hrmagozineSHRM (2013) The top workplace trends according to HR professional 1800buke streets Alexandria A 2314 USA.

Society for Human Resource Management (2013).Workplace paper: The Top Workplace Trends avail to HR professionals.

Society for Human Resource Management (2013). The top workplace trends according to HR professional 1800buke streets Alexandria A 2314 USA

Scott Cox, Tanya Goette & Dale Young (2005) Workplace Surveillance and Employee Privacy: Implementing an Effective Computer Use Policy (2005) Communication of IIMA Vol 5 Issue 2

Tengku Mohd T.Sembok (2003) Ethics of Information Communication Technology (ICT) UNESCO Regional Unit for Social and Human Sciences in Asia and Pacific (RUSHSAP) Bangkok

The Economist Intelligence Unit Ltd (2014) Closing the Skills gap: Companies and Colleges Collaborating for change.

Lauma Foundation.

United service Automobile Association (2003)

Valeniro- Devvies; J Q Singer-Vine,J (2012; December,7) The Wall Street Journal, Retrieval from htt://online.www.ws.j.com/online/sbi00004212788732478440457 8---

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

## CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

**Prospective authors of journals can find the submission instruction on the following page:** http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

## MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

## IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar