Privacy and public access: using Internet cafés in Zimbabwe

Maisiri, Esabel
Privacy and public access: using Internet cafés in Zimbabwe

Esabel Maisiri, Department of Library and Information Science, National University of Science and Technology, Bulawayo, Zimbabwe. Esabel.masiri@nust.ac.zw

Lawton Hikwa, Faculty of Communication and Information Science, National University of Science and Technology, Bulawayo, Zimbabwe. Lawton.hikwa@nust.ac.zw

Abstract
People who use Internet cafés, like any other Internet users, risk the invasion of their personal privacy. This is because the Internet has become a ‘field’ for data mining. Evidence from empirical research on the nature of the threat to personal privacy faced by Internet café users when using the Internet in a developing country was not readily available; hence this study which sought to contribute in closing this gap. The study consisted of two sections. The first section, which was guided by an individualistic definition of privacy, involved a study of Internet café operators in the City of Bulawayo, where data was collected through interviews, and an analysis of websites of some of the institutional entities in Zimbabwe. Judgemental sampling was used in both instances. Qualitative data was collected and analysed on the basis of themes that emerged from the literature. The second section was a normative assessment for postulating the way forward for Internet-based services in Zimbabwe.

The findings showed that, overall, the country was in transition, especially as evidenced by the state of the legislative regime. A data protection bill was at draft stage, and the Internet Service Providers (ISPs) did not seem to be adhering to the current legislation that required them to monitor transactions of Internet cafés; and at the same time, the Internet café operators reported that they were ignorant of the legislation that required them to observe the personal privacy of their patrons. Some of the Internet cafés had instituted measures to protect their computers and patrons while others had not bothered. The normative assessment concluded by recommending use of the communitarian position, utilitarian view and social contract theory in developing a society that respects the personal privacy of its citizens in a digital age.

Keywords: Internet privacy, Internet cafés, information ethics

Introduction
Internet cafés or cybercafés play an essential role in bridging the digital divide. They provide the general public with opportunities for both technological access and social access to the Internet (Kling, 1999 cited by Björin, Stein & Fathul, 2005). Technological access involves the provision of physical access to information technology (IT) infrastructure, computer hardware and software; and social access refers to the “mix of professional knowledge,
economic resources, and technical skills required for the use of ICTs” (Bjrørin, Stein & Fathul 2005, p. 6).

The role, extent of adoption and impact of the Internet café as a model of accessing the Internet and information by different social groups has been of interest to a number of researchers. Studies have sought, variously, to establish attributes of people who use Internet cafés, the nature of information services sought after from the Internet cafés as well as the empowering effect of Internet cafés in information access in different countries. Among these studies, Gomez (2012) provided a compilation of papers on public access to ICTs in various countries, internationally; Furuholt and Kristiansen (2007) undertook a comparison of Tanzania and Indonesia; Bjørin, Stein and Fathul (2005) focused on Indonesia and Sairosse and Mutula (2004) focused on Botswana. All such studies highlight the importance of Internet cafés in facilitating access to ICTs, information and digital communication; but many do not go further to illustrate the fact that Internet café service providers should shoulder the responsibility of protecting the rights to personal privacy of the consumers of their services when using the Internet in the service providers’ Internet cafés. Studies on the Internet and privacy have mostly focused at cyber democracy, where the Internet has been viewed as providing an alternative public sphere where the population could air its views without being subjected to the regulatory frameworks which were considered repressive in a face to face environment. Examples include Manganga (2012) who noted that “the Internet offered the possibility . . . [of an] electronic commons, a virtual public sphere” where individuals who wanted to articulate their political views freely could subvert legislation that led to reprisals by the state in Zimbabwe; and Wheeler (2007) who focused on how the Internet had allowed women in the Egyptian society, which was considered as conservative, to communicate with the outside world.

This paper, however, contends that issues of privacy and the Internet should extend further than privacy and freedom to communicate; and should include Internet privacy, that is, the privacy of the data and information which is generated by a computer in the course of someone transacting with Internet-based applications. Internet privacy has become an issue of concern because of the emergence of a “billion-dollar data collection industry devoted to obtaining personal data and leveraging it for consumer and professional purposes” (Bonadies 2013); whose activities involve data mining by tracing and capturing data on “searches, browsing histories, and social media interactions to build comprehensive profiles that trigger targeted advertisements or content”. These activities have brought serious privacy threats to Internet users. Highlighting the same concerns, Graham (1999) observed that although new technologies are presenting opportunities for massive production of digital information than could be done previously, this had raised a number of technical and social issues and is at a cost. “One possible cost is privacy” (Graham, 1999). For example, anyone who has ever used an Internet café to access their email in Bulawayo will tell you that the probability of attracting spam into one’s email account and that of addresses in their address book are very high after using an Internet Café. The need, therefore, to establish the extent to which Internet Café service providers protect the Internet privacy of their clients.

**Internet provision and Internet cafés in Zimbabwe**
According to a report by the Zimbabwe Internet Service Providers Association (ZISPA), a coordinating body of ISPs in the country, a “significant number of Internet cafés had been opened in urban centres [in Zimbabwe] . . . and some were being overwhelmed by customers” (Internet World Stats, 2011), largely using them for education and entertainment. According to Chidzero (2012) Internet penetration through Internet cafés was 5% in 2011. Harare, the capital city of Zimbabwe, had over 30 Internet cafés rising from less than 20 in a space of 2 years. The number of people with access to the Internet was estimated at almost 1.5 million, 11.5% of the population, as at December 2011, having grown from 50,000, which was 0.3% of the population in 2000; and the number for Internet Service Providers (ISP) had increased from 6 in 2003 to 27 in 2011 (Internet World Stats, 2011). The popularity and growth of Internet cafés was attributed to the fact that they presented a relatively cheap means of communication compared to phoning and also to an increase in digital literacy among college students.

The major supplier of bandwidth to private ISPs in Zimbabwe is TelOne, a government-owned communications company. Government and parastatal organisations obtain their Internet services from the Government Internet Service Provider (GISP).

In Zimbabwe, the cyberspace is regulated by the Interception of Communication Act (ICA) enacted in August 2007. The act empowers Internet and telecommunications service providers to intercept and monitor communications during transmission through a telecommunication, postal or any other related system in the country, so as to identity content that is ‘dangerous’ and poses a security risk to the country. It also requires that ISPs install technology that does the interception, including its funding and maintenance and that the ISPs provide the information so harvested to the state. ICA also provides for the establishment of a telecommunications agency, the Monitoring and Interception of Communications Centre, whose duty is to supervise the work of all the telecommunications and postal services. The Bill has been the subject of parliamentary discussions in which it is seen as violating the country’s constitution. The arguments being raised against the Bill are the same arguments that weakened the effectiveness of the Post and Telecommunications Act (2000) which preceded ICA, in regulating the cyberspace. The Post and Telecommunications Act (2000) empowered the state to monitor email usage as well as online publications and required ISPs to supply the state with information that the ISPs would have harvested, when requested to do so. This was deemed a violation of the country’s constitution in a Supreme Court ruling in 2004. After the ruling, the government instituted policy that required ISPs to renew their operating licenses with TelOne. The policy also stipulated that ISPs should report any emails that were a security risk (Manganga, 2012).

Personal privacy issues are regulated under the Access to Information and Protection of privacy Act (AIPPA) of 2002. AIPPA’s aim is to “prevent unauthorised collection, use or disclosure of personal information by public bodies: to protect personal privacy, to provide for the regulation of the mass media, provide members of the public with a right of access to records and information held by public bodies and to make public bodies accountable by giving the public a right to request correction of misrepresented personal information” (Individual Privacy Drive, 2013). AIPPA also provides for the establishment of a Media
The Information Commission whose role is to promote freedom of expression and a responsible media ([http://www.mediacommission.co.zw/](http://www.mediacommission.co.zw/)).

The legislative frameworks above have been subjected to analyses. The conclusions were that the legislations were ill-equipped to deal with the protection of personal privacy when using the Internet and social networking platforms (Manganga, 2012).

**Literature Review**

**Privacy defined**

Most authors contend that the definition of privacy is elusive (DeCew, 2012, Schafer, nd, p. 1). As a result, different conceptions of the term abound in literature. In assessing the different conceptions, DeCew (2012) pointed out that the concept of privacy is rooted in philosophy and that the term has come to assume different meanings as the focus on privacy issues from different countries and contexts increase. As a way of understanding how the different conceptions of privacy treated privacy issues, he proposed dividing the conceptions into two main categories: reductionism and coherentism. In reductionism, privacy is seen as not important in its own right; but as an issue that is subsumed or implied in other concepts, for example, rights to property. Coherentism includes various privacy issues which exhibit something of fundamental and distinctive value, and coherence to privacy interests” (DeCew, 2012). The issues pertain to privacy and control over information about self, privacy and human dignity, privacy and intimacy, privacy and social relationships, privacy and restricted access, scope of privacy and privacy is relative.

Assessing the different conceptions of privacy in literature also, Allmer (2011, p. 85) went on to call for a grounding of the conceptions in social theories because privacy is a social construct. This, he said, would provide the different conceptions with a theoretical base, which was lacking in the current definitions. He suggested grouping the definitions along the categories of social theories proposed by Fuchs (2008) (cited by Allmer, 2011, p. 85). The categories were based on how the theories “deal with the relationships of social structures and social action” (Allmer, 2011, p. 85). He came up with three groups of approaches to conceiving privacy: individualistic approaches, structuralistic approaches and the integrative approaches that combined the individualistic and structuralistic approaches.

The individualistic approaches group was based on individualistic and subjectivistic social theories which view society as being constituted by social actors and do not highlight social constraints to the action of the actors. The approaches to the conception of privacy in this group were seen as descriptive, that is, they were value neutral (Schafer, nd, p. 5). They describe the situation as is and the factors that may need to be taken into consideration. The conceptions view privacy in terms of control of information by the owners, persons or groups, of the information such that these owners are able to determine the parameters within which the information about them can be shared, and external influence is seen as invasion of privacy. Summing up the characteristics of the individualistic approaches, Allmer (2011, pp. 90-91) noted that the approaches:

... focus on the individual and understand privacy as control over information about oneself. They assume that privacy is a personal interest, or/and privacy includes the freedom from external interference in one’s personal choices,
decisions, and plans, or/and the degree of personal choice indicates how much privacy an individual has, or/and restrictions of privacy are losses, or/and privacy should be defined in a descriptive way, or/and full privacy is reached as long as the individual is able to choose which personalities should be disclosed.

The second group, the structuralistic approaches group, consist of conceptions that are based on normative principles. Their focus is on what ought to be done and not what is being done. Privacy is seen as an inalienable right which ought to be protected by law, and not an issue of individual choices. A person loses their privacy when someone else gets information about them, thus privacy denotes restricted access to an individual’s personal information. Total privacy is achieved only when there is total absence of contact with other social actors. Summing up, Allmer (2011) noted that among the structuralistic definitions, privacy is:

... a specific social structure, a moral or legal right, which is used to enable someone’s ability to limit or restrict others from access to persons or information.

The third group, integrative approaches, according to Allmer (2011, p. 92), is made up of those approaches that include both the need for protecting the people from external interference; that is, providing protection and at the same time letting the people make their personal choices. Example of authors in this group include Moor (1990; 1997) and Tavani and Moor (2001) with the Restricted Access/Limited Control (RALC) theory of privacy. The theory proposes the aspect of restricted access through the setting up of zones which individuals can use to control or limit access to their information by others, and the importance of individuals’ management of their privacy. Highlighting the double nature of the integrative-based definitions of privacy, Allmer (2011, p. 92) pointed out that:

On the one hand, these concepts recognize the constraining effects of social structures, which restrict the individual control over information. On the other hand, they also consider the individual role of control and choice, which is also required for having privacy. Integrative notions take into account that having full control over personal information can not be reached, but that individuals can limit or restrict their access because they are able to control the flow of personal information to a certain extent.

Allmer (2011, p. 93) indicated that there were some authors who questioned the whole idea of the concept of privacy. Among them are liberal thinkers who advance the notion of private property in the conception of privacy and the ‘commodification’ of privacy.

This paper assumes an integrative approach. It uses Clarke’s (2006) definition and his notion of the digital persona to assess the operations of Internet cafés as well as websites of some of the institutional entities in the country, and adopts a normative approach for postulating the way forward for the provision of Internet-based services in Zimbabwe. This is done in the discussion section.

Clarke (2006) defined privacy as “the interest that individuals have in sustaining a ‘personal space’, free from interference by other people and organisations”. In the notion of the digital persona, Clarke posited that controlling someone’s personal information is tantamount to controlling an aspect of identity which that person portrays to the world; thus, the right to
privacy “is the freedom from unreasonable constraints on the construction of own identity” (Agree and Rotenberg, 1997). In this perspective, privacy is viewed as going beyond the right to secrecy or seclusion, but that people construct their identities by selecting the personal information that they want to reveal through negotiating boundaries on the basis of a tacit moral code. This, according to Goffman means that “personal identity is not a static collection of attributes but a dynamic, relational process” (cited by Agree and Rotenberg, 1997). In sum, Clarke observed that, privacy issues centre on mechanisms that are used by people to “define themselves and conduct their relationships with one another . . . [that] comprise technologies, customs, and laws, and their reliability and fairness are necessary conditions of a just social order” (Agree and Rotenberg, 1997). Some of these mechanisms are what have been used to create a framework that has informed the first section of this study.

**Importance of privacy**

A number of authors have written on the importance of privacy. However, Clarke (2006) has succinctly grouped the issues under five perspectives: philosophical, psychological, sociological, economical and political. He noted that philosophically, human beings are “very important for their own sake” and that it is on this basis that the notions of human dignity and integrity as well as individual autonomy and self determination are considered important.

Psychologically, people need private space, be it in public or in private surroundings. This is evidenced by the fact that people tend to look around to see who is seeing them before engaging in particular behaviours.

Sociologically, Clarke (2006) noted that people should be free to behave and associate with others under the guidance of their social norms. They do not require “continual threat of being observed” (Clarke 2006).

Economically, innovators perform best when they know that they are not under surveillance. Thus, they need private space where they can freely tryout their ideas. This is supported by Lewis (2011) who saw privacy on the Internet as providing such a space.

Politically, people need to freely share their ideas and to live freely. Surveillance is contrary to democratic ideals, it stifles intellectual freedom.

**Invasion of Internet privacy**

*Surveillance*

Surveillance involves monitoring the behaviour of persons for purposes of collecting data, mostly, without the knowledge or permission of the persons. When the surveillance is limited to collecting data without monitoring the person, Clarke (1994) refers to it as dataveillance.

Commenting on surveillance, Samarajiva (1994) noted that surveillance is aimed to reduce uncertainty and increase control to the one conducting the surveillance. For a commercial entity, some of the push factors for surveillance include mass customisation in which information is required for marketing processes as well as production decision making. Surveillance threatens the privacy of the surveilled persons. This is largely because the
information collected about the persons may be manipulated with a “view to controlling their behaviours . . . the relative permanence of such records, and the relative distance between the data manipulators and customers or data subjects places the customer at a disadvantage in these relationships” (Samarajiva 1994).

Surveillance can take place in a variety of environments. Some such environments include social media platforms which have become important because of their ability to support interactivity. Thus, someone undertaking a surveillance could visit platforms used by persons they are interested in so as to establish what the persons could have posted online. Bonadies (2013) noted that employees’ private activities on social media platforms were becoming of interest to their employers because digital activities of employees can be used as a reflection of the nature of a company. As a result, employers can collect personal sensitive data about their current or prospective employees in online environments which can “help them identify character flaws or negative personality traits . . . but it also can result in privacy invasions”. He added, the worry is not about being tracked which is similar to unobtrusive observation in data collection, but when the harvested information is used to build a profile of who the person is and what they were doing, it then become an issue of invasion of the privacy of the employee.

Cyber terrorism and national security
Governments the world over are involved in surveillance programmes. Federal Bureau of Investigation’s (FBI) Carnivore programme was originally developed to find cyber terrorists; but when it was in operation, it gathered data on anyone who logged on to the Internet. It thus, ended up collecting information about everyone including those who were not terrorists. Carnivore was superseded by PRISM, which according to Snowden, the United State was using to hack into China’s database (Pempel, 2013).

Cybersecurity initiatives are inevitable, observed Lewis (2011). He said that it was the “differing views of authority, economics and the role of government [that] explain why cybersecurity initiatives so often meet with opposition from the privacy community”. He added that, at a national level, a reduction of privacy did not necessarily mean loss of civil liberties where freedom of speech is protected. He also pointed out that online surveillance presents nothing out of the ordinary because people have traditionally been sharing information, though not that widely because it was expensive in terms of time and money. What the Internet has done, is changing the economics of information sharing, it has reduced the costs. He recommended an increase in individual control on the use of data than stopping the harvesting of the data altogether.

Computer hackers and crackers
Brey (2007) said that hackers and crackers are typically highly skilled people who break into computers for “malicious purposes: to steal information and software or to corrupt data or disrupt system operations” (p. 26). He added that some hackers justify their behaviour in that it enables the sharing of data and exposes the weakness of the system broken into. Such hackers are an organised group with a code of ethics whose principles “include convictions that information should be free, that access to computers should be unlimited and total, and that activities in cyberspace cannot do harm in the real world” (Brey, 2007, pp. 26-27). He
went on to describe the different types of hacking that can be done as: cybertrespass, cybervandalism, cyberpiracy and cyberfraud. Cybertrespass happens when someone breaks into a computer system or password protected websites; cybervandalism is when someone releases malicious programmes that corrupt data on a computer network; cyberpiracy refers to as software piracy, it involves reproducing and distributing proprietary software and cyberfraud is identity theft. Cyberfraud happens when a person uses another person’s identity or a false identity as his own in an online transaction.

**Fake online researchers**

The issue of fake online researchers can also pose a threat to Internet users. These ‘researchers’ would collect data purporting to be conducting ‘innocent’ research, but end up using the collected data for other purposes.

**Pop-up advertisements on the screen with the users name and spam**

This includes unsolicited communication that is received by an online user. The communication can be a nonsense. It is confirmation that there is no privacy on the Internet.

**Possible solutions**

Solutions have been devised to help curtail some of the threats mentioned above. The solutions can be social or technical. Social solutions pertain largely to regulations and legislation on how to observe personal privacy, be it in a company or the whole country. Technical solutions involve using Privacy Enhancing Technologies on the computer to stop the tracking cookies from harvesting ones’ data. This, however, is possible where one owns the computer equipment, and not when one is depending on computers in an Internet café. Hence, the question of this study: what are the social factors on Internet privacy that affect Internet café service providers in Bulawayo, Zimbabwe, and how do they protect their clients from Internet privacy threats?

**Methodology**

The study was qualitative and descriptive. Data was collected through interviewing some of the Internet café service providers in Bulawayo and analysis of websites of some of the institutional entities in the country. The people who were interviewed were those whom the researchers were permitted to talk to. It was assumed that these were the supervisors, and not necessarily the owners. Study units were sampled using the judgemental method for the websites and the judgemental and snowball methods for the Internet cafés. Sixteen Internet cafés and twelve websites were visited. Visits to the Internet cafés were undertaken during May to June 2013 and coincided with the country’s preparations for an election at the end of July 2013. As a result, interviews were not readily granted as most of the respondents suspected the researchers to be government agents. Where possible, the data collected was validated through documentary evidence.

Analysis of data from the interview was based on the following themes:

- **Social issues - service provider perspectives**
  - Awareness of Internet patrons’ rights to privacy and business acumen.
  - Awareness and observation of regulatory frameworks that guide operations of Internet cafés and patrons’ privacy.
Influence of other players in the Internet café industry and business acumen.

Technical issues - operations undertaken
- Computer operations undertaken to ensure inaccessibility of data on users by other patrons, for example use of privacy enhancing technologies
- User training on behaviour that enhance maintenance of one’s privacy when working online.
- Physical protection of patrons.
- Signage and posters to alert patrons of the importance of maintaining their privacy when working online.

Findings
The findings are presented in two main sections. The first covers responses from the interviews conducted at Internet cafés and the second part is an observation of how some of the institutions, organisations and business entities, based in Zimbabwe have catered for personal privacy issues for their online clients and visitors.

Responses from the Internet cafés
Social issues - service provider perspectives

Awareness of patrons’ right to privacy and business acumen
A number of the respondents were aware of the need to maintain the privacy of clients, but not necessarily because it was a client’s right to have privacy when working online, but as good business and work practice.

Three respondents indicated that it was their understanding that patrons were responsible for ensuring their own privacy. Two of these respondents reported that patrons had complained of their email accounts always getting hacked each time the patrons used computers at these specific Internet cafés. However, the respondents had not been able to do much after the complaints to reverse the situation.

Awareness and observation of regulatory frameworks
None of the respondents spoken to indicated that they were cognisant of ICA or any regulatory framework that required them to ensure the privacy of their clients. It was only in one instance where the respondent indicated that they were aware that their ISP can intercept communication passing through its equipment, but did not offer their opinion on the implications of this to the Internet café patrons. However, as mentioned before, respondents may not have felt free to criticise the government since they assumed that the researchers were government agents.

Influence of other players in the Internet café industry and business acumen
The researchers were not able to establish from the respondents the existence of an association of Internet café service providers. None of the respondents said that they knew of such a body.

Technical issues - operations undertaken

Privacy enhancing activities
One of the techniques used to ensure privacy and security was to install Deep Freeze software on the network. Eleven of the respondents reported using this software, which was described as useful in eliminating “workstation damage and downtime by creating a “frozen” snapshot of a workstation’s configuration and settings” every time that the computer is restarted (Faronics, 2013). The ‘frozen’ state means that the computer was restored to its original state, that is, any changes which may have happened to the computer when it was in use are rendered ineffective, including all the history of patrons who would have been using the computer. “User and application data are re-directed to a thawed (unprotected) partition or drive enabling users to store data while still enjoying total system consistency” (Faronics, 2013). According to the respondents, Deep Freeze helped them maintain the integrity of their computers as a way of protecting both the computers and the patrons. In six of the cases, computers would automatically log-off after 5 minutes of the expiry of a patron’s booking time, activating the software. The patrons would have been sent pop-up messages to inform them of the time remaining before expiry of their booking. Two respondents said that they activated the software when they log-off their computers at the end of business each day.

Another privacy and security measure undertaken was to install a Virtual Protection Network (VNP). One respondent who was specific on the issue said that they had installed Avast VNP. VPN technologies protect data on the web by using “advanced encryption protocols and secure tunneling techniques to encapsulate all online data transfers” (Faronics, 2013).

Firewalls were another technology used. These protected data while on the computer. Three respondents said that they used firewalls to protect their machines and clients from possible hackers, prevent spam from other networks and also from websites that were a threat to security. Firewalls were essential because most of the respondents used pirated software which left their equipment with ‘cracks’, thus insecure.

Antivirus software was used by all. It helped them to detect and remove malicious software, malware. They opted for free brands, with the popular being Avast, Avira and Nod34.

In addition to the some of the technologies mentioned above, some of the respondents whose machines did not automatically log-out said that they sent pop-up messages to inform patrons that their time was about to expire and should start logging out. Where the patrons failed to do so within the stipulated time, they gave the patron a few more minutes, only to log-out; and in cases where patrons walked out without closing their accounts, the respondents did the logging out to “clear the digital footprints” as said by one respondent, before assigning a new patron at a workstation.

Viewing what a patron was doing by the service provider also emerged as another privacy concern. In one instance, the respondent said that they had set-up their network in such a way that the network administrator would only see the nodes that were active from the server and not what the patrons would be working on at their nodes. This was in contrast to another respondent who said that the network administrator was able to see what was happening on the nodes of patrons. This was important for them because they did not allow patrons to visit pornographic sites, thus were able to monitor this way.
Another security and privacy measure promoted at one Internet café was to encourage patrons to bring and use their laptops to the café. In such cases, the charges to the patrons were only for Internet use and not use of the venue, which made the rates very attractive. Such an initiative worked only where there was wireless connection to the Internet.

User training on privacy maintenance
All the Internet cafés visited never took time to explain the importance of privacy to their clients, because no one saw it as an important issue. The training that was given involved largely computer literacy skills to patrons who would have requested for the assistance.

Physical protection of patrons
Physical protection was also provided in some cases. This included shielding workstations in separate booths. The partitions were however of different heights, and at times did not provide adequate shielding in that it would be possible for other people to peep and see the computer screen in an adjacent booth while someone was working on a computer.

Physical protection measures also included, in one instance, the adoption of a ‘one person per computer’ policy. This way, the computer technicians would easily pick-out people who may be snooping around. At the Internet café where they had this policy, they did not allow even the technician to stand behind a patron who was working at a workstation, unless if the patron would have requested for the technician’s assistance.

Signage and posters
All the places visited did not have signages on the importance of maintaining online privacy.

Organisations and business entities: Internet privacy observations
Web presence has become a norm for organisations, companies and individuals in Zimbabwe, as is the trend the world over. This is largely aimed to facilitate sustained contact with stakeholders. An online search indicated that ISPs and organisations in Zimbabwe with a web presence have privacy policies. Entities visited ranged from online newspapers that include the state run newspapers like the Herald and Chronicle and privately run like the Financial Gazette, the Southern eye, to banks, commercial companies, embassies, industrial concerns, as well as personal entities like individual blogs and social networking and email accounts.

An example of an entity with a privacy policy is an ISP Utande (http://www.utande.co.zw/privacy-policy). The policy outlines the nature of information that the entity collects from Internet users who visit their site. They also state how they use the information and give the users the option to be anonymous. While the initiative by the organisation is commendable, one wonders how easy it would be for a common man on the street, whose privacy has been violated by one such organisation, to get adequate compensation when there is no law in the country that directly addresses grievances of such a nature.

Trends in the global marketing sector are also being felt in Zimbabwe as Internet-based companies whose sole purpose is online mining and harvesting of personal data for advertising and marketing are setting-up shop. An example of such a company is Icono
Global Zimbabwe (http://www.iconoglobal.com/). The company states in its privacy policy the nature of data it collects, how it collects and uses it, protects it as well as how the user’s personal rights are observed. Another example is the Marketers Association of Zimbabwe (2012). The organisation also states that its web visitors have the freedom choose between letting the organisation collect information about them or not, and that it uses the information so collected to customise its various service. It goes further in offering promotions and attractions which would make the visitors continue to use the site.

Actions stated in the personal privacy policies of the entities studied may be taken to mean that the entities are cognisant of the importance of observing the personal privacy of their clients. There, however, is need for a legislative framework that these entities can answer to. Otherwise, all that the entities may purport to do might actually be impossible to implement when the need arises.

The assessment above is confined within a physical boundary. However, it is important to note that when the public in Zimbabwe engage with the Internet, they become partakers in online activities taking place the world over. The implications are that concerns for Internet personal privacy cannot be confined to geographical boundaries.

**Discussion**

The findings above indicate a lassie-faire attitude with respect to the observation of online privacy by Internet cafés service providers in Bulawayo. This could be explained by the fact that the Internet phenomenon is, by and large, recent in the country to the generality of the population and thus, the implications of online privacy are not yet widely known. However, as part of the global village and as users of the Internet, it is imperative that Zimbabwe understands online privacy threats. An assessment of the experiences that Zimbabwe is going through in the development of legislation that adequately addresses personal privacy issues is similar to what Graham (1999) said happened in the United Stated (US). He pointed out that in the US information started being treated as an asset during the 1960s when computers began to be used to archive lots of data, both personal and governmental. The data became state property and was not accessible to the public. This was followed by public disgruntlement leading to the enactment of freedom of information legislation that gave the public access to government and corporate information, but made provisions to restrict access to sensitive information that included state secrets. Public concerns were, however, raised on the possibility of misuse of personal information under a freedom of information legislation because the legislation was not explicit about the invasion of privacy because it did not say how the personal data collected would be used. The solution was the enactment of data or privacy protection legislation. Reflecting this scenario on Zimbabwe, the freedom of information legislation tallies with AIPPA in a face to face environment, and ICA for a virtual environment. These pieces of legislation can be said to have failed to protect personal privacy, but have managed to help protect state security as shown by public disgruntlement associated with the legislation (Manganga, 2012). The government has seen this shortfall and has issued a draft Data Protection Bill. The proposed Bill provides for the establishment of an independent body, the Data Protection Authority of Zimbabwe, to administer the Bill when it becomes law. The proposed Bill makes provision for how personal data should be collected, processed and the quality maintained as well as used.
The issue of protecting personal privacy is not as straightforward as narrated above, but presents an ethical dilemma which the Zimbabwean public should address. The dilemma arises from the need to balance requirements for personal privacy and at the same time ensure the maintenance of national security. Snowden’s leak of PRISM, a National Security Agent’s surveillance programme, has raised global debate about the topic, an indication of the importance of the issue to, literally, all governments in the world (world.org).

The issue of personal privacy and national security has been of interest to a number of authors. Some of the authors and advocates for personal privacy have tended to take a rights perspective (Senges & Horner, 2009; Lewis, 2011), communitarian position and others have grounded their arguments on ethical theories (Lee 2012). The rights perspective is premised on the range of rights bestowed on citizens whose governments are signatories to the Universal Declaration of Human Rights (UDHR) (1948). Article 12 of the UDHR states that: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks” (UNESCO, 2010). According to the rights perspective, surveillance of persons by the state, even for security reasons, is a violation of someone’s right to privacy.

The rights perspective seems to be countered by the communitarian position (Communitarian Network, 1999). Communitarianism broadly, advocates for society to formulate a common understanding of the concept of good by involving all members in the society. This is because different people’s conceptions can never be universal, such that what some might consider to be for the common good may not necessarily be considered so by others, hence the need to foster a common ground that society would strive for. According to this view, if society agrees that surveillance is essential for everyone’s security, it therefore should be done.

The other approach taken in literature was to use ethical theories. The theories which have been found to be useful in resolving the personal privacy vs security dilemma include the social contract ethics, deontological ethics and consequentialist ethics, specifically utilitarianism theories (Lee, 2012). Social contract ethics which are based on the social contract theory state that humans, because of their state of nature will naturally fight for self-preservation and to promote self-interest. However, in society they get into a social contract in which they agree to forfeit their personal freedom so as to promote the safety and well-being of all. This contract forms the basis of their government. From this point of view, argues Lee (2012), “rational people would agree to monitoring . . . even if it compromises his privacy”. One can therefore say that social contract ethics supports state surveillance for security purposes.

Deontological ethics are duty-based. The view, based on Kant, is that duty is an absolute obligation and should be undertaken by everyone in the same way and that the only good thing in itself is good will and a person’s will determines the morality of an act as opposed to the outcome. The theory further states that there are hypothetical and unconditional or categorical commands or imperatives. Hypothetical imperatives apply to the ‘if . . . then situations’ and categorical imperatives are based on rules which must be obeyed by all, and
should never be violated. Categorical imperatives are centred on the fact that ‘what is right is right’. Thus, on the basis of categorical imperatives, surveillance and monitoring is wrong, irrespective of the outcome of the act.

A different view that takes into account the outcome of a behaviour is the utilitarian view, which posits that the best course of action is that which maximises the goodness of the outcome of the action. In rule utilitarianism, all rules and regulations whose outcomes give benefits that outweigh the harm that may result from applying the rules should be preferred. Basing on this view, state surveillance is preferred, although it compromises personal privacy

Conclusion

From the above discussion, it can be concluded that Zimbabwe is yet to resolve its issues on personal privacy vs national security debate. Internet cafés are as important stakeholder in this debate. It is recommended that Zimbabweans make use of the communitarian position, utilitarian view and social contract theory in developing a society that respects the personal privacy of its citizens in a digital era. Further research can focus on the public, by strata, to gather their views and at the same time create a consciousness of privacy issues.
References


