Chigona, W.

Article

Synchronised smart phones: The collision of personal privacy and organisational data security

South African Journal of Business Management

Provided in Cooperation with:
University of Stellenbosch Business School (USB), Bellville, South Africa

Suggested Citation: Chigona, W. (2012) : Synchronised smart phones: The collision of personal privacy and organisational data security, South African Journal of Business Management, ISSN 2078-5976, African Online Scientific Information Systems (AOSIS), Cape Town, Vol. 43, Iss. 2, pp. 31-40,
https://doi.org/10.4102/sajbm.v43i2.181

This Version is available at:
https://hdl.handle.net/10419/218484

Synchronised smart phones: The collision of personal privacy and organisational data security

W. Chigona, B. Robertson and L. Mimbi
Department of Information Systems, University of Cape Town,
Private Bag, Rondebosch 7701, Republic of South Africa
wallace.chigona@uct.ac.za

Received April 2011

The purpose of this study was to explore the organisational and individual motivations for incorporating personally-owned smart phones into the workplace and challenges arising from use; privacy and data security concerns of involved parties in the organisation. This study uses exploratory case study method and investigates privacy and security regarding personally-owned smart-phone usage in workplace. The study found that convenience, ease of use and access to emails were motives behind employees' use of personal smart phones in the workplace. Further, employees have higher privacy expectation. Sample for this study was small to provide statistically meaningful results, Further research is needed to cover a larger case study spanning multiple organisations in other sectors. Mobile devices are creating challenges to organisational data security and employees' right to information privacy. This study suggests that organisations need to reconsider data security and employees' privacy policies to address possible conflict between data security and employees' privacy.

*To whom all correspondence should be addressed.

Introduction

The increase in availabilty and capability of mobile phones has the valuable impact on business especially in developing countries where the availability of traditional internet is limited. In South Africa 62% of small businesses surveyed reported profit increase as a result of use of mobile phones (Samuel, Shah & Hadingham, 2005). The term 'mobile device' includes a wide range of products, but this paper focuses on smart phones. Smart phones are defined for the purpose of this report as hand-held devices that connect to a wireless or cellular network and can have software installed on them.

With the advent of smart phones, it is becoming common for employees to access organisation data through their mobile phones and synchronise their mobile phones with corporate email servers and save work-related documents (which may be confidential) onto their devices for convenient access (Goode, 2010). While this has the potential of increasing productivity and flexibility for the employees, it raises interesting privacy and security challenges for both the employee and the employer. Central to this is the question of the rights the employer has to search a personaly-owned smart phones in the event of suspected malpratices committed using the device. Data security is a complex dilemma due a myraid of legal, technical, business and social aspects that need to be considered in seeking the correct balance between these two fundamental rights. Advances in technology which are making information more mobile and transferable than ever before are compounding this even further (Reeder, Karat, Karat & Brodie, 2007). If left unaddressed, this challenge has the potential to negatively affect the impact mobile phones may have on business.

Studies in the adoption and use of mobile devices have received considerable attention for the past decade (e.g. Lubbe & Louw, 2010; Constantiou, Damsgaard & Knutsen, 2007). Nonetheless, there is still paucity of studies focusing on the use of personal smart-phones for work-related tasks. In this study, we use Price of Convinience (PoC) model to explore organisational and individual motivations for incorporating personally-owned smart-phones into the workplace. The objective of the study is to explore the problems which arise when personal information and organisation-owned information both reside on the same employee-owned device. This study addresses three specific questions:

i. What motivates employees to incorporate their personal smart phones into their worklife?

ii. What price may employees pay for using personal smart phones for work?

iii. What are employees' expectations of privacy when using personal smart phones which are used to conduct business activities?

This study contributes to practice and policy by offering with recommendations on to organisations may address the

conflicts between data security and employees'privacy. Further, this study contributes to theory building on mobile devices adoption, usage and their underlying challenges at the workplace.

Literature review

Mobile technology trends in South Africa

South Africa has one of the highest and fastest growong mobile phone penetration in Africa (Calandro, Gillwald, Moyo & Stork, 2010). In 2008, mobile phone penetration in South Africa was 90.6 mobile cellular subscription per 100 inhabitants (ITU, 2010). There is also a growing trend in the use of mobile phones within organisation. According to World Wide Worx (2005), mobile phones were a close second to laptops computers, with 93% of corporations intended to deploy among employees in 2005. There is also a growing trend in the use of Smart phones by corporates with 75% of the corporates already using smart phones in their organisations in 2010 (Jamsa, 2010).

Mobile devices in the workplace

Increasingly employees are using their personal mobile phones to access business data (Credant Technologies, 2007; Harmer, Pauleen & Schroeder, 2008). Harmer *et al*., (2008) found that employees feel a greater sense of self-worth when they are given the freedom to conduct business activities on their personal mobile devices. Similarly, Besseyre des Horts and Isaac (2006) noted that field workers expressed feelings of responsibility and prestige when using mobile technologies for work and felt that increased mobility enabled them to be more professional and acquire more responsibilities. The study found that one of the main reasons for the increasing use of personally-owned mobile devices is that organisations often only issue mobile phones to management level. The sense of prestige may vary depending on proffession. For example, in the study by Dearman and Pearce (2008) an academic group embraced the concept of mixing business and personal data on personal mobile devices. The group from industry, in contrast, showed various reasons for wanting to separate work and personal data but in practice had difficulty doing so.

Credant Technologies (2007) found that smart phones were the second most common device after flash drives used for storing data. However, the majority in the Credant Technology study felt that the use of iPods in the workplace represented an immediate threat to corporate data security. However, even though there was an understanding of the threat posed by iPods to the organisation, 49% of the respondants felt that they would not implement any security policies until they were sure that mobile devices were more widely used to store corporate data.

The extent of data loss through mobile devices is not known. According to the Computer Crime and Security Survey, only 4% of respondants reported a theft or loss of proprietry data from mobile devices, while 8% reported a theft or loss of customer data from mobile devices (Computer Security Institute, 2008).

Privacy and data protection

There are a number of theories of privacy, however, their defintions of privacy are not all encompassing (Tavani, 2007). Tavani (2007) proposes the Restricted Access / Limited Control (RALC) Theory which defines an individual as having privacy:

"in a situation with regard to others [if] in that situation the individual ... is protected from intrusion, interference, and information access by others" (Tavani, 2007: 10).

The South Africa Constitution defines privacy or "Informational Privacy" (Eiselen, Pistorius, Roos & Van der Merwe., 2006: 313) or "Data Protection as:

"*... the right not to have their person or home searched, their property searched, their possessions seized or the privacy of their communications infringed*." (Eiselen *et al*., 2006: 353).

Informational privacy is, therefore, achieved when one has control of his or her personal information (Eiselen *et al*., 2006).

Expectation of privacy

An individual's right to privacy is not absolute and in some exceptions the rights to privacy may be limited (Collier, 2002; Eiselen *et al*., 2006). In the context of mobile phone communications, users consider their mobile phones personal and private; same was as a handbag or a wallet (Chatfield & Hakkila, 2005). Chatfield and Hakkila (2005) found that users percieved voice communications, emails, pictures and Short Message Services (SMS's) as having different levels of privacy.

The South African Constitutional Court perceives an individual's expectation of privacy as a continuum with one's personal and intimate life at the one end and communal or business life at the other end (Eiselen *et al*., 2006). A person's expectation of privacy would then decrease along the continuum as one moved further away from the personal domain (Eiselen *et al*., 2006). Employees and employers both have rights to privacy which are recognised by Constitutional Court of South Africa (Collier, 2002). Employers have legitimate requirements for wanting to monitor or intercept employees' personal communications which take place in the general course of business (Lease, 2005). Similarly, the Constitutional Court of South Africa points out that an employee cannot be expected to have no right to privacy in the workplace (Collier, 2002). Employees will always be entitled to some level of privacy, meaning that the employer cannot force an employee to relinquish all rights to privacy (Collier, 2002). Therefore, the employer needs to clearly differentiate between what is considered private and what is considered business related data (Collier, 2002).

Theoretical models

We identified two theoretical models relevant to this study, the Resitricted Access/Limited Control (RALC) Theory and

PoC. The former was used as a theoretical lens when considering the requirements for an effective mobile device usage policy that respects the employee's right to privacy. The latter was used as a framework to understand the the use of mobile technologies at work.

The restricted access / limited control theory

RALC theory can be applied in developing an online privacy policy by addressing three principles: the concept, the justification and the management of privacy (Tavani, 2007). Instead of defining privacy in terms of control over information, Tavani (2007) defines an individual as having privacy when one is protected from intrusion, interference and information access by others. Individual do not need complete control over personal data to manage their privacy. Rather, a limited control in respect of choice, consent and collection of personal data is required (Tavani, 2007).

The RALC Theory acknowledges that "zones" of privacy exist to protect access to personal information (Tavani, 2007). This is consistent with the South African Constitutional Court's opinion that a person expectation of privacy would decrease along a continuum as one moved further away from the personal domain (Eiselen *et al*., 2006).

The rice of convenience model

The PoC Model developed by Ng-Kruelle, Rebne, Swatman and Hampe (2002) has been used in a series of studies (e.g. Shumarova & Swatman, 2006; Ng-Kruelle, Swatman, Hampe & Rebne, 2006) to understand the effects of external factors on the adoption behaviours of users of mobile innovations. Ng-Kruelle, Rebne, Swatman and Hampe (2003) used the model to understand the price that consumers must pay in terms of their privacy for the convenience of mobile commerce applications such as Global Positioning System (GPS) based location aware services. Ng-Kruelle *et al*. (2003) consider how attitudes to three different aspects of privacy have changed over time, namely: information privacy, telecommunications privacy and privacy vs. security. Their study showed that privacy desensitisation can occur over time as a result of the various factors i.e. the ones used in the PoC Model.

The PoC Model (see Figure 1) consists of four first-order variables:

- Society: represents the values and ideologies of the employees of the organisation (Ng-Kruelle *et al*., 2002).
- Government: represents the laws regarding an employees right to informational privacy (Ng-Kruelle *et al*., 2002).
- Industry: represents the manufacturers of mobile devices and the influence that they have on the users attitudes towards the adoption of mobile technologies (Ng-Kruelle *et al*., 2002).
- Company: represents the employer and the the employer's own PoC calculus of weighing up the convenience of having a mobile and productive work force against the costs of having less control of corporate data (Ng-Kruelle *et al*., 2002).

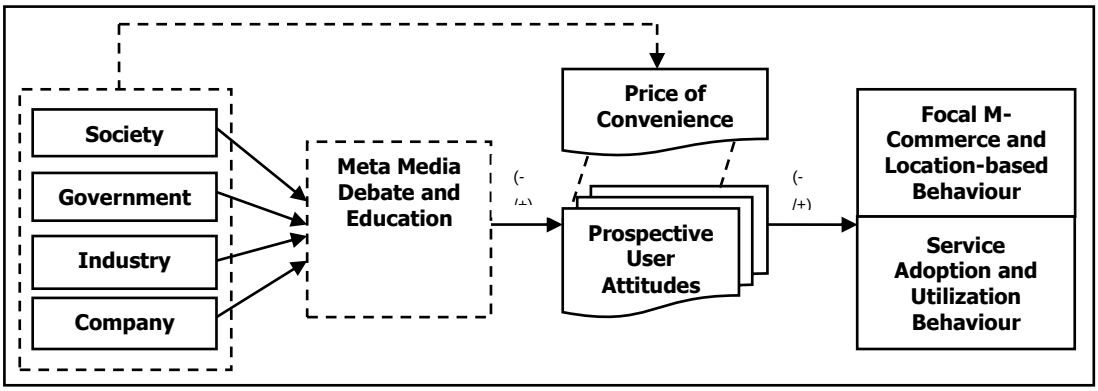

Figure 1: The PoC Model (Ng-Kruelle *et al*., 2002)

Over and above each directly affecting variables the individual's PoC calculation, the first-order also act as the input to the second-order variable, the "Media". The "Media" represents the effect that the media has on the perceptions of the employee through information and education (Ng-Kruelle *et al*., 2002).

"Prospective User Attitudes" is the net influence of all the first-order and second-order variables and is directly linked to an individual's PoC calculus (Ng-Kruelle *et al*., 2002). Ng-Kruelle *et al*. (2002) in their Weberian socioeconomic analysis of PoC sensitivity distinguish between three different types of "Prospective User Attitudes", namely: PoC Sensitive, PoC Calculative and PoC Insensitive groups of people. PoC Sensitive individuals are highly sensitive with regard to their potential loss of privacy when deciding on performing the required task. PoC Calculative individuals are pragmatic when deciding and PoC Insensitive individuals showed little concern for their loss of

privacy. The PoC Calculative individuals group is the fastest growing group of the three (Ng-Kruelle *et al*., 2002).

PoC in the context of this study is the price that the employee must pay in terms of the privacy of personal data for the convenience of having access to business and personal data on a single mobile device (Ng-Kruelle *et al*., 2003). The organisation also has a price to pay in terms of data security for the convenience of having a productive and mobile workforce. The PoC Model is suited for this research because it recognises the various socio-economic and technological influences that affect an individual's motives and behaviour when considering the adoption of mobile technologies (Ng-Kruelle *et al*., 2003).

Research methodology

We adopted an interpretive stance to investigate the concept and social aspects of mobile devices usage at workplace. Our qualitative, cross-sectional, exploratory case study research method included interviews and standard case study techniques. This method is an appropriate way to research an area in which few previous studies have been carried out as it allows in depth interrogation of the relationships in a particular situation (Benbasat, Goldstein & Mead, 1987). The investigation allowed us to focus on the employee use contexts of the smart phones and the underlying employee' motives towards using a personal smart phone for work-related tasks (Abbott, 1990). The data was collected in August and September 2009. Semi-structured interviews were used as a primary data collection method and computer usage policies pertaining to different functions in the organisation were used as secondary source of data.

As suggested by Klein and Myers (1999), we adhered to the requirements of systematic gathering; and reliable recording and transcription of data to guarantee the validity of the empirical observations. We selected the respondents as per 'sampling for heterogeneity' criteria (Miles & Huberman, 1994). All respondents were selected from the Risk Advisory and Group Information Systems departments of a South African organisation. Two sample groups were identified for the interviews. The first group (see Table 1) was a purposive, non-probability sample consisting of three specifically selected experts in the fields of cyber-forensics, cyber-law and computer security.

Table 1: Sample group 1

Position	Expertise
Director – Risk Advisory	Cyber-forensics and Cyber-law
Senior Manager – Risk Advisory	I.T. Security
Senior Manager – Group Information Systems	I.T. Security

The second group, comprising of six respondents, was a convenience sample of mobile device users within the organisation. The only prerequisite was that they synchronised their personal mobile devices with the corporate network. Potential subjects were pre-screened to identify suitable candidates. The sample had even split of three male and three female respondents. Their experience of using the device ranged from four month to six years at the time of the interview.

Interview procedures

The interviews were semi-structured and comprised of open-ended questions derived from mobile device literature, privacy literature, prior research studies, and the unique technological aspects related to mobile technology. Interviews were audio recorded and then transcribed. All identifying names and places were removed to maintain confidentiality.

Data analysis

All interviews were transcribed and studied together with the existing literature, applicable legislations and computer usage policies obtained from the organisation. Categories and themes identified in the interview transcripts were analysed for the various constructs mentioned in the RALC theory and the PoC model.

We prepared the raw data files and read the transcripts in detail to fully understand the details of the text (Thomas, 2003). We then created categories and themes from the transcripts. Segments of text were identified in the transcripts and coded into different themes or meaning units. We used data analysis software Welt QDA to assist in the coding of themes and categories by automatically grouping similar codes from various transcripts together.

Case description

The sampled organisation was a large South African organisation that offered financial advisory services. The identity of the organisation is withheld for ethical reasons. The organisation's currently subsidised mobile phones for all management level staff. The managers were free to choose any device or contract and paid the difference in cost. This policy relieved the organisation of any responsibilities regarding the management of the mobile devices and their associated accounts. However, this also meant that the mobile devices were considered personal devices and, therefore, not under the control of the organisation.

All employees were allowed to synchronise their mobile devices with the corporate network, even if the mobile devices were personally-owned. Although most smart phones were supported on the corporate network, it was found that at the time of data collection technical support for Blackberry smart phones had been discontinued. This meant that a group of people that previously synchronised their smart phones with the network and were now unable to continue doing so. The Blackberry users were still included into the sample for the study.

The organisation was chosen as a case for this study because all employees were allowed to use smart phones in the workplace regardless of their positions in the organisation. This facilitated compliance to sampling for heterogeneity. Further, the organisation's business focus on financial

services rendered then a suitable venue for investigation collission of personal privacy and security of corporate data.

Results

Impact of media on perceptions

The respondents were asked if they could recall how the media might have had influenced their decision to use their personally-owned smart phones for business purposes. Most respondents recalled advertisements on various brands of mobile smart phones and cited convenience and easy access to emails as key advantages highlighted by the media. These findings support the mobile adoption theory that the media plays a role in the adoption process (Ng-Kruelle et al., 2002). However, some respondents claimed that the media only served to provide general information, but did not influence their decisions to use the technology. For instance, a respondent said "... the media influences you in terms of making things look very easy". However, her decision on which smart phone to buy "...came ... from my husband". Similarly, another respondent said "It [the media] definitely helps by reminding people of the advantages, that's not the reason why I bought it, but their marketing plays a big role".

The respondents were asked if they were aware of any information regarding data security on mobile devices in the media. Most respondents were more familiar with information about laptop security. Other respondents indicated that they have seen data security sections in IT and Information security websites, but felt that such websites targeted individuals who work in IT security industry and not normal users.

Employees' motivation for synchronisation

Convenience was noted as one of the main rmotivations for the respondents using smart phones to synchronise with email and calendar services. The convenience arose primarily due to the seamless internet connection, and spontaniaty i.e. access to personal and business emails without having to spend the time starting up a laptop and connecting to the internet using a 3G card. Three partipants expressed frustartions associated with process of logging on and connecting to email using a laptop as a time consuming. Examples of statements attributable to convinience are:

"...just to be connected at the airport or something - you would have to open your notebook up, put your 3G card in and fire up the whole machine, there was not often time for that - but now it is so easy. It really is a time saver..."

"It's convenient, it's always with you. The mail interface on this thing is as close as you are going to get it to your notebook. It's easy, it's on the fly, you can see anything I need to see on my notebook I can see on my smart phone."

Portability and access anywhere functionalities that smart phones provide which are almost similar to desktop and laptop computers were also cited as drives.

All respondents expressed a general underlying need to be more accessable via email as their primary motivation for using a smart phone. A respondent said "I like having constant access because you often get urgent emails that need a response relatively quickly."

Further, all respondents agreed that access to business emails via their smart phones greatly increased their ability to stay on top of things. Most respondents could relate to the findings of Besseyre des Horts and Isaac (2006) which concluded that using mobile technologies for work enganders feelings of responsibility and prestige for employees. They felt a sense of higher responsibility and all respondents felt that fast and easy access to their emails enabled them to perform their duties more professionally.

Challenges employees faced in using smart phones

Employer expectation and work-life balance

The respondents felt that their superiors expectations on their availability to perform work-related tasks changed once they become aware that the employee had access to emails after work hours and that the employees could still work away from office and after office hours.

"I've had instances when it comes to Monday morning and the boss says, 'Where is that thing that I asked you for?' and then I check my mail and he sent me the mail Saturday morning. So I just tell him that is an unrealistic expectation."

Another respondent explained "...it can start to create an expectation that by downloading your emails that you are willing to action them." A respondent also felt that "It can create the expectation that you are online all the time..."

However, employer expectation varied directly with the rank of the employee in the organisation.

All respondents indicated that they accessed work emails in their personal time beyond office hours. Most of them felt this was a negative aspect of synchronise ther Smart Phones with work but felt it was so innevitable. Some of the responses were:

"Work doesn't stop, weekends are just time spent away from the office still working - unfortunately."

"You've always got work after hours. It interrupts the social life. But nowadays work dominates your life anyway."

Respondents explained the challenges of juggling the constant access to emails with their other personal demands.

"I am a mom of two small children so I do not want people to have the expectation that when I am at home I can just quickly draw up a proposal between the hours of 7 and 12 at night. I do other stuff, and over the weekend, I commit myself to my family."

Some respondents developed strategies to regain control over their personal time and control when they accessed

their business emails. One respondent deactivated the automatic synchronisation with the corporate email server, "I don't have the automatic send/receive on, and I will manually synchronise it once or twice at night to see what comes through". However, senior management and directors felt they were being more agile and respond to work related emails in a timely manner and were supposed to be available 24/7. This result supports the findings by Cousins and Varshney (2009) in which they found blurring boundary between work and home life.

Separating business from personal data

The ability to separate business from personal data is increasingly becoming important (Middleton & Cukier, 2006). Most respondents used the same mobile phones for both work and private data storage. A respondent felt that he "...would find it difficult and admin intensive to separate work and personal info on a device like a mobile phone." A respondent claimed that although folder management capabilities were available on smart phones, they were often difficult to use and further, different applications had their own default location for storing data on the device.

Two respondents suggested that they would consider using two separate smart phones to separate work from personal data. A respondent added that "...because there is this whole grey area..." regarding privacy and data security, that the organisation was reconsidering the option of issuing a organisation-owned mobile device in the same way it did with laptops.

Employee's expectation of privacy

The respondents were asked to rate themselves as 'Privacy Sensitive', 'Privacy Calculative' or 'Privacy Insensitive'. Only one respondent rated himself as 'Privacy Sensitive' and stated that he "...would require a high level of privacy ..." for all types of data. Two respondents regarded themselves to be 'Privacy Insensitive'. One of them said "Definitely insensitive, so long as I don't lose anything". Three respondents regarded themselves as 'Privacy Calculative', and felt that they would carefully assess anything that affected their rights to data privacy. A respondent stated that she "would consider all aspects and conceptualise a solution to the problem."

Most respondents had a high expectation of privacy regarding their personal mobile devices inspite of storing organisation data on their mobile phones. However, a respondent indicated that he would allow a certain level of access to specific folders.

"I take a whole bunch of photos that I don't want work [colleagues] seeing. May be if they have a specific rule on a specific folder that you keep work stuff on, and they can look at that folder, but otherwise no"

There appeared to be different levels of privacy expectations depending on whether the device was personally-owned or was owned by the organisation. The respondents' expectation of privacy on their organisation-issued laptops was different to that of a personally-owned device. However, it was noted that the definition of organisation-owned property could be contested. For example, an IT Manager commented that "...a month after we've issued the laptops to the guys, it's now their laptop". Some respondents expected that a certain amount of privacy be granted to them on their work laptops. A respondent felt that "I think we need to have privacy despite being in the working environment". Others had a limited expectation of privacy when using organisation-owned equipment. "...so long as it is on a company asset your privacy is second to what the company wants."

The findings support those of Chatfield and Hakkila (2005) in that respondents acknowledged having different levels of privacy regarding the different types of data that may be stored on a mobile device. Personally-owned mobile devices are likely to contain more personal data than business data, and are more likely to be used in a personal context. The protection of this personal private data such as casual SMSs, personal emails and photographs may have caused the employees to be protective over their personal devices.

Searching organisation-owned equipment

Most respondents understood and acknowledged the limitations placed on their right to privacy when using organisation-owned equipment. Although the policy was in line with the legal requirements for searching organisation-owned equipment, the need to enforce those rights did not happen often. A Senior Manager –Risk Advisory said "In the 11 years that I've been with the company, it has happened twice that I got asked to investigate someone's computer, so it's not common". The organisation's Electronic Communications Policy (ECP) offered some level of assurance regarding the unnecessary invasion of an employees' privacy by prohibiting the use of the organisation's communication systems for any kind of electronic snooping without proper cause and authorisation. The prohibition specifically included system administrators and supervisors. "...so it's not a case of, we get your machine at the helpdesk and scratch around. We must have proper procedure in place to go have a look...". The policy on General Rules made provision for its application to personally-owned devices used to access the organisation's network, but to date had never been enforced.

Searching personally-owned equipment

The analysis of the expectation of privacy regarding personal devices shows the challenges involved which would arise when searching personally-owned devices, even if the device was known to be synchronising with the corporate network. Most respondents indicated that they were not willing to have their personal mobile phones be searched and considered this as invasion of privacy.

The responses from a respondent regarding how they would feel if communications sent or received from a personally-owned device while being connected to the organisation's network were intercepted, suggested that there would be considerable resistance. A respondent said he would "not very happy! I think it would be considered an invasion of privacy". However, he added that that only in the event of;

"...a criminal investigation", would consider it a valid reason to search or intercept communications sent or received from a personally-owned device.

The respondents said they could only allow if the search was extended to a "specific folder other than personal folder". This was in line with the organisation's policy, which required that employees have a personal folder for personal data on organisation-owned equipment. With regard to this challenge, a respondent suggested the use of "Anton Piller order" to gain access to personally-owned smart phone when it was suspected that it contained data belonging to another person or an organisation. An Anton Piller order is only issued in extreme circumstances where it can be shown that an urgent intervention is neccessary to preserve important documents which may be destroyed (Hofman, 2006).

Organisation's computer usage policies

Employee right to privacy

Every employee was required to sign the organisation's ECP as part of the employment process. The ECP stated that:

"Although incidental and occasional personal use of the Firm Communication Systems is permitted, users automatically waive any claims to privacy."

The policy stated that any personal communication that was intended to be confidential should rather be sent via an alternative means. The requirement to waive any claims to privacy was in stark contrast to the Constitutional Court's opinion that an employee cannot be expected to have no right to privacy in the workplace whatsoever (Collier, 2002). There was also some level of employee's right privacy when using organisation-owned equipment. "We extend the courtesy for you to create a private folder for yourself, so we won't go and snoop if there's no justification for it." (Senior Manager, Risk Advisory).

Further, the ECP stated that:

"The Firm reserves the right to access and disclose the contents of a users electronic and ..., but intends to do so only when it has a business reason." (ECP).

This provision was in line with the Communication-Related Information Act 70 of 2002 (RIC Act) which provided for the interception of indirect communications provided there was a valid business reason and that the employee gives full consent. In fact, each time an employee logged on to their computer, they electronically assigned the organisation"...the right to monitor and intercept ANY communications (whether sent or received)." (Network Log on Notification.)

The employees' right to privacy was also acknowledged in the organisation's Policy on Hand Held Devices, which contained a section related to the employee's right to personal privacy.

Data security policy

The Policy on Protecting Information stated that all data stored on Universal Serial Bus (USB) media storage devices should be encrypted. According to the organisation, USB media included memory sticks and external hard drives. Although smart phones were not explicitly listed, they would be classified among as a USB storage device. The policy stated that all computer and communication devices, including smart phones required a password or Personal Identification Number (PIN) code to access organisation data. Most of the respondents had not been enforcing the security measures in full. Some claimed that "... too frustrating to put in a PIN every time one is accessing the mail server from the smart phone". This security mechanism was only enforced on the server side. "The biggest issue is that people don't lock their [smart phones] when they are done ... The phone locks itself but everyone puts it on the maximum, which is 60 minutes."

The Policy allowed contact information, email messages and calendar items to be downloaded to a mobile. However, the actual adherence to this policy could not be enforced mainly because the organisation was forced to relax the security measures to accommodate the different makes of smart phones that needed to be connected to the network.

Employee awareness of computer usage policies

A banner which appeared when one logged in the organisation network summarised the organisation's computer usage policies and set out specific guidelines on private use. A hyperlink from the banner led to a page with a complete set of computer usage policies on the organisation network. However, most respondents had a little idea of the content of the policy; "I think I have actually read it and it deals with privacy and the organisation's rights to your computer". A respondent said she was unsure on some of the rules and policies but continued to say that "I think they are on the side where they respect our privacy a great deal compared to other companies". Only a respondent recalled the detail contained in the click through banner.

Discussion

Conflict between the organisation's security policies and the employees' right to privacy

The organisation's computer usage policies limited the employee's expectation of privacy regarding personal communications in the workplace. The policies pertained specifically to organisation-owned computer equipment including mobile devices which were issued by the organisation. The policies also included any personally-owned device used to connect to the organisation's computer network. The employee's right to informational privacy, personal privacy, and their right to protection against the disclosure of personal information were all acknowledged and respected in the organisations policies.

Employee's personally-owned mobile device is perceived as personal as a handbag or a wallet. As such, employees'

expectation of privacy regarding personally-owned devices was far greater than that of an organisation-owned device. The difference in expectations of privacy between personally-owned devices and organisation-owned devices therefore means that the organisation's computer usage policies cannot simply be extended to include personally-owned devices. A separate policy that specifically caters for the unique characteristics of personally-owned devices should be drafted (Hunter, 2007).

Dealing with risks associated with leaking of sensitive data via smart phones

The organisation's policies regarding data security were clear and extend to include data stored on personally-owned devices. These policies dealt with various security measures that should be implemented and the types of data which may be synchronised with a mobile device. However, these policies were not easily enforced due to the different types of devices that needed to connect to the network. A solution to the problem would require the manufacturers of smart phones can agree on a common security standard (Bellavista, Xie & Tugcu, 2009). Until the time that such a standard is agreed upon, a pragmatic solution would be to limit the access to organisation network only to those devices the organisation can manage.

A respondent said "...we need to have a policy that defines what the organisation's tolerance level is and what it aims to protect". A policy that specifically caters for the use of personally-owned devices needs to be implemented (Hunter, 2007). More importantly, however, Goode (2010) suggests that employees need to be educated regarding the organisation's policies on the use of personally-owned devices. When the employees' awareness of the organisation's policies is low, an appreciation of the risks involved in storing data on portable devices is less likely to be considered.

Use of mobile phone evidence during disciplinary proceedings

Evidence obtained by means of intercepting business emails sent or received using a personally-owned mobile device using the organisation's email server would be easy to obtain with limited infringment on the employee's right to privacy. This is because physical access to the device is not nessesary and the information can be obtained from the organisation's server. On the contrary, an organisation may have limited authority to obtain such evidence from a personal mobile device and would have to use some legal mechanism, such as the execution of an Anton Piller order to justify the need to invade someone's privacy to that extent. Ultimately, the pragramatic option to get access to such data would be to have a policy which ensures that the organisaton sctualy owns the mobile devices. However, provision of organisation owned mobile phones to employees may be costly impractical both for the organisation and the employees.

Conclusion

Our findings show that the convenience of using smart phones and having easy access to emails could be the strong motivations which influence the adoption and use of smart phones in South African. The pressures from employers to perform in the workplace as well as the personal desire of motivated employees to succeed and climb the corporate ladder also may also add to the growing phenomenon.

Based on the level of usage, it may be said that the benefits that smart phones offer to both the employee and the organisation seem to outweigh the disadvantages. Employer and employee both walk a fine line of trust and respect where employees are trusted to respect the data that they work with, while employers are expected to respect the employee's right to privacy. If this balance is respected, then there can exist a freedom where employees can take full advantage of smart phone technology.

Organisations have a responsibility for ensuring the security of sensitive data. The growing importance of data security, and the increased computing power that employees can carry around in their pockets together with the limited access that the organisation has to personally-owned devices should cause organisations to rethink their data security policies. Issuing employees with corganisation-owned smart phones is cumbersome, but remains one of the few ptions available. There is, therefore, need for more effort to educate and inform mobile device users on how to be more security conscious.

The South African legal framework regarding privacy and data protection provides for the development of effective computer usage policies. However, an individual's right to privacy is a fundamental right, and one which is highly protected. For an organisation to accomodate the growing tide of personal device usage in the workplace, there needs to be a simple mechanism by which personal data and business data can be separated. This would require that the ownership of data be defined and identified at a technically fundamental level to allow for the automatic extraction of relevant data from any device whether owned by the organistion or not. By reducing the need for human intervention, an organisation can reduce the relative infringement on an individual's right to privacy, thereby regaining a greater control over the security of its data.

Due to the limited sample, it was not be meaningful to provide statistically meaningful results. The study serves to provide insight into the phenemena of collission of personal privacy and organisation data security. Further studies are necessary to adress the generalisability of the findings.

References

Abbott, A. 1990. 'A primer on sequence methods', *Organisation Science*, **1**(4): 375–392.

Bellavista, P., Xie, J. & Tugcu, T. 2009. 'Recent advances in mobile middleware for wireless systems and services', *Mobile Network and Applications*, **14**(1): 1–3.

Benbasat, I., Goldstein, D.K. & Mead, M. 1987. 'The case research strategy in studies of information systems', *MIS Quarterly*, **11**(3): 369–386.

Besseyre des Horts, C. & Isaac, H. 2006. 'Adoption and appropriation: Towards a new theoretical framework. An exploratory research on mobile technologies in French companies*', d'information Et Management*, **11**(2): 9-50.

Buyukkokten, O., Garcia-Molina, H., Paepcke, A. & Winograd, T. 2000. 'Power browser: Efficient web browsing for PDAs'. **In** *Proceedings of the SIGCHI conference on human factors in computing systems, 1-6 April 2000*, pp.430–437.

Calandro, E., Gillwald, A., Moyo, M. & Stork, C. 2010. 'Comparative sector performance review 2009/2010'. **In** *Towards evidence-based ICT policy and regulation, Volume Two*. Policy Paper 3. Research ICT Africa.

Chatfield, C. & Hakkila, J. 2005. 'It's like if you opened someone else's letter — User perceived privacy and social practices with SMS communication'. **In** *Proceedings of the seventh international conference on human computer interaction with mobile devices and services*, Salzburg, Austria, pp.219-222.

Collier, D. 2002. 'Workplace privacy in the cyber age', *Industrial Law Journal*, **23**: 1743-1759.

Computer Security Institute. 2008. 'Computer crime & security survey.' [online]
URL: http://i.zdnet.com/blogs/csisurvey2008.pdf. Accessed 22 April 2011.

Constantiou, I. D., Damsgaard, J. & Knutsen, L. 2007. 'The four incremental steps toward advanced mobile service adoption,' *Communications of the ACM***, 50**(6): 51-55.

Cousins, K. & Varshney, U. 2009. 'Designing ubiquitous computing environments to support work life balance', *Communications of the ACM*, **52**(5): 117-123.

Credant Technologies. 2007. 'Survey on portable storage devices: iPods, what you don't secure could hurt you. [online] URL:http://www.credant.com. Accessed 22 April 2011.

Dearman, D. & Pierce, J.S. 2008. 'It's on my other computer! Computing with multiple devices'. **In** *Proceeding of the twenty-sixth annual SIGCHI conference on human factors in computing systems - Displayful and displayless*, Florence, Italy, pp.767-776.

Eiselen, S., Roos, A., Pistorius, T. & Van der Merwe, D. 2006. *Information and communications technology law*. Durban: LexisNexis.

South Africa, 2002. *Electronic Communications and Transactions Act 25 of 2002 Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002*. Pretoria: Government Printer.

Fulk, M. 2001. 'Improving web browsing on handheld devices'. **In** *Proceedings of ACM CHI extended abstracts on human factors in computing systems*, Seattle, Washington, pp. 395–396.

Goode, A. 2010. 'Managing mobile security: How are we doing?', *Network Security*, **2010**(2): 12–15.

Harmer, B., Pauleen, D.J. & Schroeder, A. 2008. 'Cause or cure: Technologies and work-life balance'. **In** ICIS 2008 Proceedings. Paper 163. [online]
URL:http://aisel.aisnet.org/icis2008/163. Accessed 22 April 2011.

Hofman, J. 2006. 'Electronic evidence in South Africa'. [online] URL:http://lawspace.law.uct.ac.za. Accessed 22 April 2011.

Hunter, P. 2007. 'Is now the time to define a mobile security policy', *Computer Fraud and Security*, **6**: 10-12.

International Telecommunication Union (ITU). 2010. 'Telecommunication/ICT development report'. [online] http://www.itu.int/ITU-D/ict/publications/wtdr_10/index html . Accessed 26 March 2012

Jamsa, P. 2010. 'Mobile marketing trends: Smartphones conquering Africa?*'* [online] URL: http://internationaldigitalmarketing.com/2010/10/29/mobile-marketing-trends-smartphones-conquering-africa/. Accessed 22 April 2011.

Klein, H.K. & Myers, M.D. 1999. 'A set of principles for conducting and evaluating interpretive field studies in information systems', *MIS Quarterly*, **23**(1): 67–92.

Lease, D. 2005. 'Balancing productivity and privacy: Electronic monitoring of employees.' Paper presented at the European Management and Technology Conference, Rome, Italy, June 2005.

Lubbe, B. & Louw, L. 2010. 'The perceived value of mobile devices to passengers across the airline travel activity chain', *Journal of Air Transport Management*, **16**(1): 12-15.

MacKay, B. 2003. ' "The gateway": A navigation technique for migrating to small screens.' **In** *Proceedings of CHI*, Fort. Lauderdale, Florida, USA, pp. 384–385.

Middleton, C.A. & Cukier, W. 2006. 'Is mobile e-mail functional or dysfunctional? Two perspectives on mobile e-mail usage', *European Journal of Information Systems*, **15**(3): 252-260.

Miles, M.B. & Huberman, A.M. 1994. *Qualitative data analysis: An expanded sourcebook*. California, Thousand Oaks: Sage Publications.

Ng-Kruelle, G., Rebne, D.S., Swatman, P.A. & Hampe, J.F. 2002. 'The price of convenience: Privacy and mobile commerce', *Quarterly Journal of Electronic Commerce*, **3**(3): 273-286.

Ng-Kruelle, G., Rebne, D.S., Swatman, P.A. & Hampe, J.F. 2003. 'The price of convenience: Developing a framework for analysing privacy sensitivity in the adoption of wireless applications.' **In** *Proceedings of 16th BLED International Conference on Electronic Commerce, June 9-11, Bled, Slovenia*.

Ng-Kruelle, G., Rebne, D.S., Swatman, P.A. & Hampe, J.F. 2006. 'Biometrics and e-Identity (e-passport) in the European Union: End-user perspectives on the adoption of a controversial innovation', *Journal of Theoretical and Applied Electronic Commerce Research*, **1**(2): 35-56.

Reeder, R.W., Karat, C., Karat, J. & Brodie, C. 2007. 'Usability challenges in security and privacy policy-authoring interfaces'. *Lecture Notes in Computer Science* vol 4663/2007, pp. 141-155.

Samuel, J., Shah, N. & Hadingham, W. 2005. 'Mobile communications in South Africa, Tanzania and Egypt: Results from community and business surveys'. [online] http://www.vodafone.com/assets/files/en/AIMP_09032005.pdf. Accessed 10 April 10, 2011

Shumarova, E.V. & Swatman, P.A. 2006. 'The new economy, e-value and the impact on user acceptance of pervasive IT'. **In** *Proceedings of 19th Bled eConference eValues, Bled, Slovenia*.

Tavani, H.T. 2007. 'Philosophical theories of privacy: Implications for an adequate online privacy policy', *Metaphilosoph*, **38**(1): 1-22.

Terre Blanche, M., Durrheim, K. & Painter, D. 2006. *Research in practice: Applied methods for the social sciences.* Cape Town: UCT Press.

Thomas, D. 2003. *A general inductive approach for qualitative data analysis.* Auckland: New Zealand: School of Population Health. University of Auckland.

Varshney, U. & Vetter, R. 2002. 'Mobile commerce: Framework, applications and networking support', *Mobile Networks and Applications*, **7**(3):185-198.

Waycott, J. & Kukulska-Hulme, A. 2003. 'Students' experience with PDAs for reading course materials', *Personal Ubiquitous Computing*, **7**(1): 30–43.

World Wide Worx. 2005. 'Laptops rule corporate investment in mobility'. [online] URL:http://www.worldwideworx.com/2005/02/09/laptops-rule-coporate-investment-in-mobility/. Accessed 22 April 2011.

Yue, W., Mu, S., Wang, H. & Wang, G. 2005. 'TGH: a case study of design natural interaction for mobile guide systems', **In** *Proceedings of the seventh international conference on human–computer interaction with mobile devices and services Mobile HCI*, Salzburg, Austria, pp. 199–206.