South African Journal of Information Management
ISSN: (Online) 1560-683X, (Print) 2078-1865

Towards a conceptual framework for protection of personal information from the perspective of activity theory

Authors:
Tiko Iyamu[1]
Yandiswa Ngqame[2]

Affiliations:
[1]Department of Information Technology, Cape Peninsula University of Technology, South Africa

[2]Department of Business Administration, Cape Peninsula University of Technology, South Africa

Corresponding author:
Tiko Iyamu,
iyamut@cput.ac.za

Dates:
Received: 22 Mar. 2017
Accepted: 20 June 2017
Published: 06 Nov. 2017

How to cite this article:
Iyamu, T. & Ngqame, Y., 2017, 'Towards a conceptual framework for protection of personal information from the perspective of activity theory', *South African Journal of Information Management* 19(1), a867. https://doi.org/10.4102/sajim.v19i1.867

Background: Personal information about individuals is stored by organisations including government agencies. The information is intended to be kept confidential and strictly used for its primary and legitimate purposes. However, that has not always been the case in many South African government agencies and departments. In recent years, personal information about individuals and groups has been illegally leaked for other motives, in which some were detrimental. Even though there exists a legislation, *Protection of Personal Information (POPI) Act*, which prohibits such malpractices, illegally leaked information has however, not stopped or reduced. In addition to the adoption of the *POPI Act*, a more stringent approach is therefore needed in order to improve sanity in the use and management of personal information. Otherwise, the detriment that such malpractices cause too many citizens can only be on the increase.

Objectives: The objectives of this study were in twofold: (1) to examine and understand the activities that happen with personal information leaks, which includes why and how information is leaked; and (2) to develop a conceptual framework, which includes identification of the factors that influence information leaks and breaches in an environment.

Method: Qualitative research methods were followed in achieving the objectives of the study. Within the qualitative methods, documents including existing literature were gathered. The activity theory was employed as lens to guide the analysis.

Result: From the analysis, four critical factors were found to be of influence in information leaks and breaches in organisations. The factors include: (1) information and its value, (2) the roles of society and its compliance to information protection, (3) government and its laws relating to information protection and (4) the need for standardisation of information usage and management within a community. Based on the factors, a conceptual framework was developed.

Conclusion: This study can be used to guide implementation of information protection acts in any environment. It empirically contributes to societal awareness on how and why personal information is leaked and breached. Also, it will benefit academic domain, particularly in the use of activity theory.

Introduction

Many organisations depend on, and regard information as an important resource in their activities (Beshears et al. 2015). In some organisations, information is considered as having the same value as people and money (White 2007). In both private and government organisations, individuals are required to provide information about themselves, for various reasons, such as remuneration, skill development and departmental demographics. Similarly, information is collected about clients and customers (Mithas, Ramasubhu & Sambamurthy 2011). According to Geder and Dmytrenk (2015), most individuals are not aware of how this information is processed, stored, used, protected or disposed.

Many organisations are confronted with information control challenges, such as personal information breaches (Norberg, Horne & Horne 2007; Van der Aa et al. 2015). Information is leaked for various reasons by employees and external forces. Based on empirical studies, internal employees are involved in most of the incidents of information security breaches that takes place in organisations (Garba, Armarego & Murray 2015; Mohammed, Ronda & Shereeza 2015; Norman & Yasin 2013). It is noted that personal information is either leaked or sold for financial benefit (Haynes 2006). This type of behaviour leaves organisations with negative reputation (Casandesus-Masanell & Hervas-Drane 2013).

Directly or indirectly, employees are involved in information security breaches in their organisations (Kaushal, Khan & Kumar 2015). D'arcy, Hovav and Galletta (2008) argue that many cases of information breaches does occur as a result of an employee's negligence, who fails to follow organisation's regulations and policies. This type of negligence can happen at any time and at any level of an organisational structure. Also, such negligence can happens while organisations are increasingly interested in careful management of private information.

Breach or leak of personal information can be detrimental to the concerned individual. If and when this problem is not well managed, it poses potential threats to the rights of citizens (Borena, Belanger & Ejigu 2015). To avoid such threat to citizens' rights, regulations and policies are formulated by organisation and government promulgates legislative bills and acts. However, implementation and practice of the policies, bills and acts are activities that are carried out by individuals and groups, which makes them even more challenging. Nilsen et al. (2013) suggest that challenges are attributed to roles and responsibilities of individuals who are tasked with the implementation of policies.

Activities within social systems are well illustrated by activity theory (AT), from both technical and non-technical perspectives. AT is a conceptual framework that is based on the idea that an activity is primary to social systems or environments (Hashim & Jones 2007). The theory is known to be a powerful and clarifying descriptive tool rather than a strongly predictive theory. The main objective of the AT is to understand the unity of consciousness and activity, which it clarifies that consciousness is located in everyday practice (Nardi 1996).

Thus, the objective of this study was to understand how and why personal information is leaked and to examine the factors that influence such actions. AT was employed as a lens in the analysis. This paper is structured into six main sections. The first and second sections presents a review of existing work on protection and breaches of personal information and AT, respectively. The third section covers the approach that is employed in the study. The findings from the analysis are discussed in the fourth section. In the fifth section, we present how human actions are reproduced through activities, in a conceptual framework. Finally, a conclusion is drawn in the sixth section.

Protection and breaches of personal information

Information is always needed and used whether in small or large, public or private organisations. Organisations gather information about their services, products and individuals including that of their competitors. The information is collected from various sources, based on their requirements and purposes. Thereafter, the sets of information are analysed, controlled and managed over a period of time, for different reasons (Dinev et al. 2013). What is even more challenging is how the information is used, which include concerns about privacy, security and breaches. Young and Quan-Haase (2013) suggest that users disclose information because they have made a conscious effort to protect themselves against potential violations.

The essentiality of information is in its criticality which is based on the fact that it enacts the identity and association of individuals, groups or entities. According to Brandimarte, Acquisti and Loewenstein (2013), this includes any type of information that links or identifies individuals or group of individuals. In this context, some attributes of information includes names, identity numbers, place of birth, medical and financial accounts (Carlson 2016). Personal information is mostly used in organisations, private or public. In some terms, information is regarded as a currency and the most valuable asset of an organisation, because its value continues to increase (Casandesus-Masanell & Hervas-Drane 2013; Norman & Yasin 2013).

Due to the fact that information privacy is in everyone's interest, about 103 countries, including South Africa and Brazil, promulgated laws to protect personal information (Mohammed et al. 2015). However, compliance or adherence to those laws of personal information protection remain a challenge. Landau (2015) in his work emphasis on the need for compliance with laws and regulations, which prevents unethical behaviours in a country. Individual's compliance and management of compliance are activities that are carried out within contexts, such as information privacy.

Information privacy is one of the most critical subjects that affect individual's rights, which sometimes manifest into negative outcome in some activities that are performed by organisations, whether private or public. It is therefore a serious problem for many organisations in that how information privacy is managed affects and influences their reputation and the services that they provide. At a larger scale, the world acknowledges information privacy as a basic human right within a democratic society (Acquisti, John & Loewenstein 2013). In some perspectives, information and communication technology (ICT) is blamed for information privacy breaches and threats (Mills et al. 2009). This concludes that privacy of information cannot be fully achieved in an organisation without policy and compliance to the policy (Davis & Squibb 2014). Information technology is used to enable, support and manage the use, accessibility and control of information privacy in many organisations. According to BeVier (1995), the roles of ICT in the management of information include storing, processing and receiving information and dissemination to relevant stakeholders or parties.

Information protection is an activity that organisations take seriously, in order to prevent loss and unauthorised access and information disclosures. Such activity is often regarded as the main aspect of ensuring respect for private life (Acquisti, Brandimarte & Loewenstein 2015). As a result, many organisations formulate information security measures

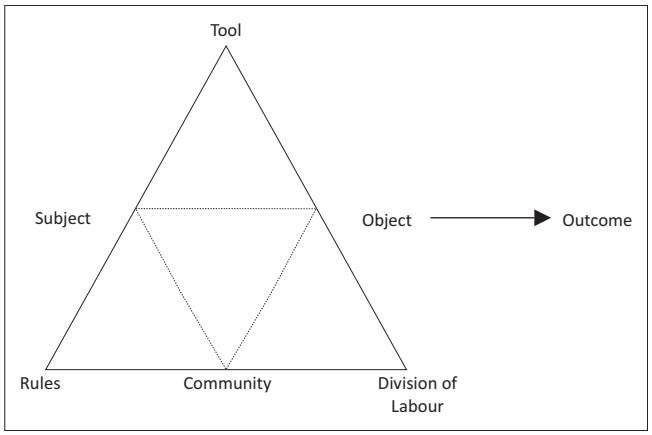
and regulations, which are intended to prevent information threats and losses. This is within the notion and premise that without policies and regulations, an organisation can experience incidents of information leakages and breaches (Deng et al. 2011). Thus, roles, responsibilities and accountabilities of information usage by employees should be well guided (Posey et al. 2013).

Activity theory

Activity theory (AT) focuses on human interaction and the use of tools within a social system. As shown in Figure 1, the theory consists of six main components, which include tools, objects, division of labour, community, rules and subject. Waitoller and Kozleski (2013) view activity as a complex social organisation, which consists of: (1) tools such as computers; (2) subjects, such as internal employees and clients; (3) rules, such as policies, norms and regulations that surround employees; (4) community, which comprises groups or units of employees or stakeholders; (5) divisional labour, which includes co-workers and colleagues who help in reaching outcomes; and (6) the objects, which forms part of organisational sustainability. AT describes an activity as being composed of subject, object and tools as a mediator. According to Karanasios and Allen (2013), an activity is anything small or big that we do, which is based on assumptions that tools mediate between subject and object.

Technology is seen as tools that facilitate social action and interaction within context (Hashim & Jones 2007). The processing of information involves interaction between the user and tools, such as technology. The theory explains the interaction that takes place between human beings and social system, which include working environment and community of people.

From an AT perspective, for an activity to take place there has to be a subject, which is driven by a motive (Karanasios & Allen 2013). Private and governmental departments require individuals to surrender personal information in order to receive service (Mohammed et al. 2015), and this information is processed by employees and stored manually or digitally in order to retain its confidentiality, integrity and availability (Wylie et al. 2000). There are policies and regulations that must be adhered to, when handling information, including the *Protection of Personal Information Act* (*POPI Act*; South African Government 2013). Organisational staff and colleagues represent the community, while division of labour are individual employees in an organisation with their post profiles. The outcomes are expected to help prevent challenges that are faced by organisations in handling private information of their clients.



Source: Engeström, Y., 2001, 'Expansive learning at work: Toward an activity theoretical reconceptualization', *Journal of Education and Work* 14(1), 133–156. https://doi.org/10.1080/13639080020028747

FIGURE 1: Engeström's expended activity theory model.

The research approach

In order to achieve the aim of the study, which was to understand and examine the activities that influence personal information leaks, towards the development of a conceptual framework, qualitative research methods were employed from the perspective of the interpretivist approach. Biedenbach and Müller (2011) argue that the interpretivist approach assumes a subjective reality in that things are socially viewed and constructed from different perspectives. According to Bryman (2012), the qualitative research methods focus on the explanation and expression of opinion and view, rather than quantification in the collection and analysis of data. The study did not depend on statistical data, rather on qualitative meanings associated to things (Webley 2010). The qualitative research methods rely on human perceptions, and an understanding within contexts (Berger 2015; Myers 2013). Bocconi, Kampylis and Punie (2013) based their qualitative study on desk research, which entails collection and analysis of existing literature. The methods and approach were selected for this study on these basics.

Based on the premises as presented above, the research question was formulated: what are the factors that influence information breaches and leakages in an organisation? Within the context of this research question, a review of existing literature in the areas of information leakages including *POPI Act* was carried out. The study therefore focuses on examining the factors that influence leakage of personal information. The analysis was conducted, using the AT as a lens.

Activity theory analysis and discussion

Activities that concerns sharing of personal information were analysed and discussed, as presented herewith. This was done from an AT perspective, following its tenets: tools, subject, rules, community, division of labour and object:

- ***Activity theory: Tools*** – different tools are used to store, retrieve, use, disseminate and manage information within an environment. In the context of information, three main types of tools exist in many private and public organisations: (1) cabinets, which contain hardcopy of files; (2) shelves and boxes, where files are kept; (3) computer and other electronic devices, such as discs that

store softcopies of documents and files. These tools are employed differently by individuals and organisations, to store and manage information. The use of the tools depend on operational and strategic intent of an individual organisation. Therefore, the tools require different methods of uses, for storage and accessibility.

- Organisations employ various techniques and methods in using tools to protect information from leakage and theft. The offices and store rooms where hardcopies of files are kept are normally locked for security and protection purposes. Some offices are guarded by personnel refers to as security guards. In addition, some organisations have extra security measures, which include closed-circuit television monitoring and alarm systems.
- However, the same tools that are used to host, secure and protect personal information from leakages and theft in an organisation can also be used for accessibility. The accessibility can either be for the interest of the organisation or for malicious purposes, consciously or unconsciously. According to Hayashi et al. (2013), various tools, such as electronic devices can be used as facility for information leakage. The tools do not use themselves, but are used by human beings, directly or indirectly.
- ***Activity theory: Subject*** – In AT, subject is a living being, referred to as actor, which can either be internal and external personnel in an organisation or society. Internal personnel include employees at any level of an organisation. External personnel consist of clients, business partners and other associates and stakeholders who are not part of internal employees. The personnel undertakes different roles and responsibilities concerning information in their organisations.
- Information leakage or protection is an action performed by human beings, consciously or unconsciously. Activity about information leakage or protection is carried out by any of the actors that are associated with the environment, irrespective of their roles or capacity. According to Malandrino et al. (2013), employees begin to make better decisions towards controlling their privacy as they learn more about information leakage. This type of awareness prompts formulation of rules for governance purposes within environments.
- ***Activity theory: Rules*** – in every organisation including the society at large, there are rules, which include policies, norms and regulations. These rules are formulated and promulgated by actors who also live within the social system. The same actors are obliged to conform to the rules that are produced in carrying out their activities. However, the compliance of society (subject) is based on the type of information (object), policies and rules.
- Rules concerning personal information leakage or projection are formulated or circulated in order to maintain sanity within an environment. These rules therefore defines the merit and demerit of actions that leads to information storage, access, use and management within an organisational environment. The rules are intended to ensure credibility and sanity in the accessibility and use of personal information. Yang et al. (2013) argue that dissemination of personal information in itself does not necessarily indicate privacy leakage, it depends on whether the action was intentional or unintended. Also, such dependency is influenced by the context of the community where the action is performed.
- ***Activity theory: Community*** – a community is a social system, which can be an organisation or within a society. Thus, a community comprises of groups of people in a social system. In an organisation, this includes groups or units consisting of employees or stakeholders. Each community is defined or formed in accordance to common or allied interest. A community is therefore a network of people that is formed for specific purpose. Thus, the information that is meant for a community is intended to be accessed or shared by all of its members, which often have both negative and positive consequences. Lasecki, Teevan and Kamar (2014) suggest that information could be posted to a group without knowing that private or sensitive information is being leaked.
- As members of a community interact, using devices, they intentionally or unknowingly share private information. Also, members of a community sometimes make use of the same devices for their collaborative activities. Through these actions, information about a community member can be leaked to other members within a network. According to Raval et al. (2014), devices can leak private information, if not properly cleaned such as personal pictures and enterprise secrets when sent to a group.
- ***Activity theory: Division of labour*** – this is the act of sharing an activity among actors, for a common goal or objective. The division entails workers or employees in the same community contributing to an activity in reaching outcomes. Tasks are allocated to employees in accordance to their skills, knowledge and experience, which become their source of power to make a difference to an activity, such as information care.
- In the division of labour, actions are produced and reproduced in order to carry out individual and group tasks of an activity, to store, access, secure and manage personal information. Thus, accessibility is critical and should be defined by specific needs. Accessibility to any type or volume of information should be driven by user permission (Raval et al. 2014).
- ***Activity theory: Object*** – the object is the outcomes that are produced and reproduced by actors within a community. The actors make use of various available tools in different ways towards achieving their objectives. The outcomes are not always positive, irrespective of the intentions. When outcomes are positive, it helps the organisation with sustainability, competitiveness and reputable drive. However, outcomes are sometimes negative, which manifest from conscious or unconscious actions of actors within an environment.
- There is information about each human activity. The information is stored or disseminated or both, within context and for specific purpose. What is even more important is the type of information that is gathered, stored and accessed. Some types of information are more

sensitive than others, which influences their accessibility and security. Towards improved management, it is important to know who discloses or shares sensitive or personal information, and the motives behind such actions.

Based on the above, it is clear that information security and privacy require collaboration and implementation through the government's legislative act and an organisation's policies and regulations. The policies and regulations will guide individuals' activities in the prevention and breaches from unauthorised access and use of information. Internal employees' unethical practices, such as access and use of unauthorised information, cause severe damage to an organisation's information system (Suar & Khuntia 2010).

Towards conceptual framework for protection of information

Implementation of policies and regulation on information security and privacy are fundamental from three perspectives: (1) to reduce the risk of information breaches (Urey 2015); (2) increase control of information security (D'arcy, Hovav & Galletta 2008); and (3) improve the integrity of customer information (De Koker & Jentzsch 2013). From the analysis and discussion that is presented above, we found four critical factors that can be used towards development of information protection and breaches conceptual framework. The factors include: (1) information and its value; (2) the roles of society and its compliance to information protection; (3) government and its laws relating to information protection; and (4) the need for standardisation of information usage and management within a community. As shown in Figure 2 (conceptual framework), the factors are interrelated and influences protection or leakage of personal information. The discussion that follows helps to gain better understanding of the conceptual framework.

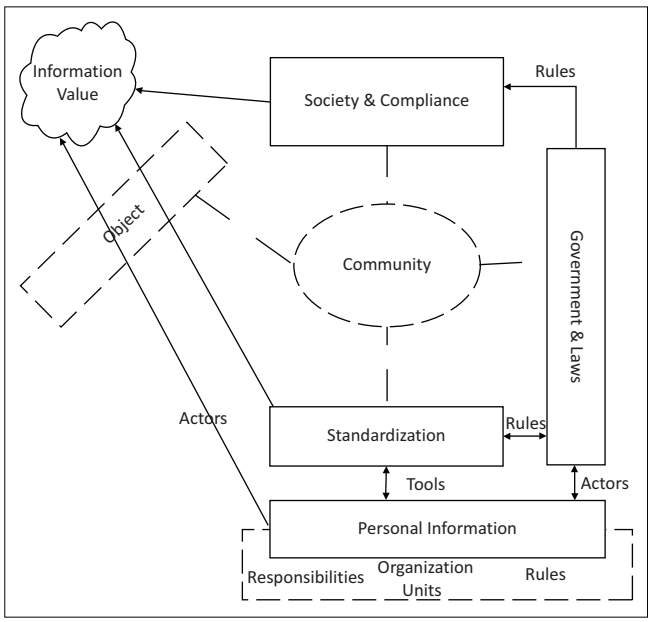


FIGURE 2: Framework for protection of information.

Information and value

Every information is considered valuable. This is attributed to the fact that information plays an important role in protecting valuable assets of an organisation. These assets involve any information that is kept by the organisation, whether processed, recorded or stored (Davis & Squibb 2014; Von Solms & Van Niekerk 2013). Thus, every bit and piece of information is useful primarily because together they form an entity, which makes a different in an environment. As bits and pieces of information are refined and analysed, the value shapes and defines the environment. However, it depends on the community and the actor who's got access to the information. Also, the perceived usefulness of information is based on the need or motive of the actor who accesses the information and how it was accessed. As documented and revealed in this study, there are rules and regulations that are meant to protect information from unauthorised access and use. However, there are still instances of leaks, unauthorised access and use of personal information within communities. This could be attributed to intended and unintended actions.

People intentionally leak or disseminate unauthorised information for various reasons. Some of the reasons could be associated with selfish interests, monetary exchange and malicious acts. Others share personal information unknowingly and ignorantly. These types of actions can be ascribed to how the policies are understood and interpreted.

Society and compliance

Information is often considered valuable and powerful by individuals and society in general, at all times. Hence, there is need for information security practice, to protect information of individuals and an organisation at large, whether it is organised or processed (Garba et al. 2015). As such, confidentiality of information is always high on the agenda of many organisations, irrespective of the business focus. As a result, policies, rules and regulations are formulated within society including government administrations and agencies.

Compliance to rules and regulations is useful in reducing uncertainty within a society. Also, compliance helps to improve decision-making among individuals and groups during societal activities. Information is stored electronically to enable and ensure availability, accessibility, integrity, credibility and its confidentiality. In many organisations, there are several policies in the form of legislations, regulations and guidelines that influence good handling of information. Hence, information governance sets out guidelines and accountability controls to ensure good information compliance that need to be adhered to.

Government and laws

Privileged and few countries including South Africa enjoy the right to access information. The importance of this right is that it acknowledges the value of activities, such as accountability, responsiveness and openness. It permits

public access to any information held by the state (Peekhaus 2014). Section 32 of the South African constitution promotes right of access to any information held by the state through the *Promotion of Access to Information Act "PAIA" of 2000*. The "PAIA" Act gives an individual or group of individuals a right to formally lodge a request from the information officer, without breach or leak.

In South Africa, there is also the *POPI Act*, which was promulgated in 2013. The Act was primarily proclaimed to protect personal information. It therefore focuses on information privacy, both in government and private organisations within boundaries of the country.

Standardisation

Some information breaches are caused by know-how or influenced by the settings of the environment. Information breach is found to have different meanings to different actors in various situations (Malandrino et al. 2013). To many people, information privacy is the right to prevent disclosure of personal information (Cox, Goette & Young 2015; Mani et al. 2015). According to Heirman, Walrave and Ponnet (2013), information privacy is a claim made by individuals to determine when, how and to what extent can their information be made available.

Standardisation helps to guide and maintain a common understanding amidst various meanings of information privacy and security. Also, there are numerous activities that are performed by actors, which necessitates standardisation to avoid chaos and instil discipline in the accessibility and use of information concerning individuals. Thus, the International Organisation for Standardisation (ISO) designed and developed a code of conduct labelled ISO 27002, for practices, which are to protect information security in organisations. The ISO code of conduct's role is to emphasise on the importance of information security within an organisation. ISO 27002 takes cognisance that confidentiality and non-disclosure agreement cannot be compromised (Jašek, Králík & Popelka 2015; Peltier 2013).

Conclusion

The study inspects how and why personal information can be leaked in any environment. The study also examines the factors that influence such actions. As revealed in the study, the same tools that are used to host, secure and protect personal information can also be used for its accessibility in an organisation. Access to information can either be for personal or organisational interest, for positive or malicious purposes. Thus, this study can be of interest and benefit to both academic and organisation including government agencies.

This paper makes contributions in three perspectives, theoretical, methodological and practical. The theoretical contribution is the paper's addition to existing literature, to increase the relevance of information privacy literature to academics, organisations and the society in general. The study methodologically advances the use of AT in information systems (IS) studies. The paper practically contributes through its foundation for building a conceptual framework, which can be used to minimise chances of personal information leaks and breaches. Also, the conceptual framework can be used to examine a model that will enable the *POPI Act* in government administrations and agencies.

The study can be used for generalisability in that the conceptual framework can be applied to different environments. However, there are limitations in this study in that it was not experimental. Thus, future research can be conducted, using the conceptual framework presented in this paper, to guide an empirical study and examine a model that will enable the *POPI Act* in government and agencies.

Acknowledgements

Competing interests

The authors declare that they have no financial or personal relationship(s) that may have inappropriately influenced them in writing this article.

Authors' contributions

T.I. was responsible for articulating the research problem, design, analysis and writing the article and N.Y. for gathering the literature that were used in the study.

References

Acquisti, A., Brandimarte, L. & Loewenstein, G., 2015, 'Privacy and human behavior in the age of information', *Science* 347(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Acquisti, A., John, L.K. & Loewenstein, G., 2013, 'What is privacy worth?' *The Journal of Legal Studies* 42(2), 249–274. https://doi.org/10.1086/671754

Berger, R., 2015, 'Now I see it, now I don't: Researcher's position and reflexivity in qualitative research', *Qualitative Research* 15(2), 219–234. https://doi.org/10.1177/1468794112468475

Beshears, J., Choi, J.J., Laibson, D., Madrian, B.C. & Milkman, K.L., 2015, 'The effect of providing peer information on retirement savings decisions', *The Journal of Finance* 70(3), 1161–1201. https://doi.org/10.1111/jofi.12258

BeVier, L.R., 1995, 'Information about individuals in the hands of government: Some reflections on mechanisms for privacy protection', *William & Mary Bill of Rights Journal* 4, 455.

Biedenbach, T. & Müller, R., 2011, 'Paradigms in project management research: Examples from 15 years of IRNOP conferences', *International Journal of Managing Projects in Business* 4(1), 82–104. https://doi.org/10.1108/17538371111096908

Bocconi, S., Kampylis, P. & Punie, Y., 2013, 'Framing ICT-enabled innovation for learning: The case of one-to-one learning initiatives in Europe', *European Journal of Education* 48(1), 113–130. https://doi.org/10.1111/ejed.12021

Borena, B., Belanger, F. & Egigu, D., 2015, 'Information privacy protection practices in Africa: A review through the lens of critical social theory', in *2015 48th Hawaii International Conference on System Sciences (HICSS)*, pp. 3490–3497.

Brandimarte, L., Acquisti, A. & Loewenstein, G., 2013, 'Misplaced confidences privacy and the control paradox', *Social Psychological and Personality Science* 4(3), 340–347. https://doi.org/10.1177/1948550612455931

Bryman, A., 2012, *Social research methods*, 4th edn., Oxford University Press, New York.

Carlson, R.C., 2016, *The new rules of retirement: Strategies for a secure future*, John Wiley & Sons, London, England.

Casandesus-Masanell, R. & Harvas-Drane, A., 2013, 'Competing with privacy', *Management Science* 61(1), 229–246. https://doi.org/10.1287/mnsc.2014.2023

Cox, S., Goette, T. & Young, D., 2015, 'Workplace surveillance and employee privacy: Implementing an effective computer use policy', *Communications of the IIMA* 5(2), 6.

D'arcy, J., Hovav, A. & Galletta, D., 2008, 'User awareness of security countermeasures and its impact on Information Systems misuse: A deterrence approach', *Information Systems Research* 20(1), 79–98. https://doi.org/10.1287/isre.1070.0160

Davis, D.C. & Squibb, J., 2014, 'Policies, procedures and devices used by US hospitals for HiPPA privacy security compliance', *Communications of the IIMA* 4(2), 7–16.

De Koker, L. & Jentzsch, N., 2013, 'Financial inclusion and financial integrity: Aligned incentives?', *World Development* 44, 267–280.

Deng, M., Wuyts, K., Scandariato, R., Preneel, B. & Joosen, W., 2011, 'A privacy threat analysis framework: Supporting the elicitation and fulfilment of privacy requirements', *Requirements Engineering* 16(1), 3–32. https://doi.org/10.1007/s00766-010-0115-7

Dinev, T., Xu, H., Smith, J.H. & Hart, P., 2013, 'Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts', *European Journal of Information Systems* 22(3), 295–316. https://doi.org/10.1057/ejis.2012.23

Engeström, Y., 2001, 'Expansive learning at work: Toward an activity theoretical reconceptualization', *Journal of Education and Work* 14(1), 133–156. https://doi.org/10.1080/13639080020028747

Garba, B.A., Armarego, J. & Murray, D., 2015, 'Bring your own device organisational information security and privacy', *ARPN Journal of Engineering and Applied Sciences* 10(3), 279–1287.

Geder, M.G. & Dmytrenko, A., 2015, '8 steps to effective information lifecycle management', *Information Management*, 32–35.

Hashim, N.H. & Jones, M.L., 2007, 'Activity theory: A framework for qualitative analysis', in *Proceedings of the 4th International Qualitative Research Convention (QRC)*, PJ Hilton, Malaysia, 03–05 September.

Hayashi, Y.I., Homma, N., Mizuki, T., Aoki, T., Sone, H., Sauvage, L. & Danger, J.L., 2013, 'Analysis of electromagnetic information leakage from cryptographic devices with different physical structures', *IEEE Transactions on Electromagnetic Compatibility* 55(3), 571–580. https://doi.org/10.1109/TEMC.2012.2227486

Haynes, A.W., 2006, 'Online privacy policies: Contracting away control over personal information', *Penn State Law Review* 111, 587.

Heirman, W., Walrave, W., & Ponnet, K., 2013, 'Predicting adolescents' disclosure of personal information in exchange for commercial incentives: An application of an extended theory of planned behaviour', *Cyberpsychology Behaviour, and Social Networking* 16(2), 81–87. https://doi.org/10.1089/cyber.2012.0041

Jašek, R., Králík, L. & Popelka, M., 2015, 'ITIL and information security', in *Proceedings of the International Conference on Numerical Analysis and Applied Mathematics 2014*, No. 1648, AIP Publishing, Rhodes, Greece, 22–28 September.

Karanasios, S. & Allen, D., 2013, 'ICT for development in the context of the closure of Chernobyl nuclear power plant: An activity theory perspective', *Information Systems Journal* 23(4), 287–306. https://doi.org/10.1111/isj.12011

Kaushal, A., Khan, A. & Kumar, V., 2015, 'Big data: A brief investigation on different privacy issues', *International Journal of Innovation & Advancement in Computer Science* 3(1).

Landau, S., 2015, 'Control use of data to protect privacy', *Science* 347(6221), 504–506. https://doi.org/10.1126/science.aaa4961

Lasecki, W.S., Teevan, J. & Kamar, E., 2014, 'Information extraction and manipulation threats in crowd-powered systems', in S. Fussell, W. Lutters, M. Morris & M. Reddy (eds.), *Proceedings of the 17th ACM Conference on computer supported cooperative work & social computing*, ACM, New York, 15–19 February, 2014, pp. 248–256.

Malandrino, D., Petta, A., Scarano, V., Serra, L., Spinelli, R. & Krishnamurthy, B., 2013, 'Privacy awareness about information leakage: Who knows what about me?', in A.R. Sadeghi & S. Foresti (eds.), *Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society*, ACM, Berlin, Germany, 04–08 November, pp. 279–284.

Mani, D., Heravi, A., Choo, K.K.R. & Mubarak, S., 2015, 'Information privacy concerns of real estate customers and information security in the real estate industry: An empirical analysis', in I. Welch & X. Yi (eds.), *Proceedings of Australasian Information Security Conference (ACSW-AISC 2015)*, Sydney Australia, Commonwealth of Australia, Sydney, 27–30 January, pp. 53–56.

Mills, A., Chen, R., Lee, J. & Raghav Rao, H., 2009, 'Web 2.0 emergency applications: How useful can Twitter be for emergency response?' *Journal of Information Privacy and Security* 5(3), 3–26. https://doi.org/10.1080/15536548.2009.10855867

Mithas, S., Ramasubhu, N. & Sambamurthy, V., 2011, 'How information management capability influences firm performance', *MIS Quarterly* 35(1), 237–256.

Mohammed, D., Ronda, M. & Shereeza, M., 2015, 'Cybersecurity challenges and compliance issues within the US healthcare sector', *International Journal of Business and Social Research* 5(2), 55–66.

Myers, M., 2013, *Qualitative research in business and management*, 2nd edn., Sage, London, Britain.

Nardi, B.A., 1996, 'Activity theory and human-computer interaction', in *Context and consciousness: Activity theory and human-computer interaction*, pp. 7–16, viewed 13 February 2016, from https://wiki.cc.gatech.edu/ccg/_media/people/dan/quals/nardi-ch1.pdf

Nilsen, P., Ståhl, C., Roback, K. & Cairney, P., 2013, 'Never the twain shall meet? A comparison of implementation science and policy implementation research', *Implementation Science* 8(1), 63. https://doi.org/10.1186/1748-5908-8-63

Norberg, P.A., Horne, D.R. & Horne, D.A., 2007, 'The privacy paradox: Personal information disclosure intentions versus behaviors', *Journal of Consumer Affairs* 41(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Norman, A.A. & Yasin, N.M., 2013, 'Information systems security management success factor: Retrospective from the scholars', *African Journal of Business Management* 7(27), 2646–2656.

Peekhaus, W., 2014, 'South Africa's promotion of access to information act: An analysis of relevant jurisprudence', *Journal of Information Policy* 4, 570–596. https://doi.org/10.5325/jinfopoli.4.2014.0570

Peltier, T.R., 2013, *Information security fundamentals*, CRC Press, Taylor & Francis Group, London, United Kindom.

Posey, C., Roberts, T., Lowry, P.B., Bennett, B. & Courtney, J., 2013, 'Insiders' protection of organisational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors', *MIS Quarterly* 37(4), 1189–1210.

Raval, N., Srivastava, A., Lebeck, K., Cox, L. & Machanavajjhala, A., 2014, 'Markit: Privacy markers for protecting visual secrets', in A.J. Brush, A. Friday, J. Kientz, J. Scot & J. Song (eds.), *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*, ACM, Seattle, WA, 13–17 September, pp. 1289–1295.

South African Government, 2013, *Protection of Personal Information Act*, viewed 15 March 2017, from http://www.gov.za/documents/protection-personal-information-act

Suar, D. & Khuntia, R., 2010, 'Influence of personal values and value congruence on unethical practices and work behavior', *Journal of Business Ethics* 97(3), 443–460. https://doi.org/10.1007/s10551-010-0517-y

Urey, C.J.L., 2015, *European safe harbour privacy policy customer information*, viewed 15 March 2017, from http://www.techtarget.com/wp-content/uploads/files/clientresources/ttgt_eu_safeharbor_privacy_policy.pdf

Van der Aa, H., Leopold, H., Mannhardt, F. & Reijers, H.A., 2015, 'On the fragmentation of process information: Challenges, solutions, and outlook', In *International Conference on Enterprise, Business-Process and Information Systems Modeling*, pp. 3–18, Springer International Publishing.

Von Solms, R. & Van Niekerk, J., 2013, 'From information security to cyber security', *Computers & Security* 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Waitoller, F.R. & Kozleski, E.B., 2013, 'Understanding and dismantling barriers for partnerships for inclusive education: A cultural historical activity theory perspective', *International Journal of Whole Schooling* 9(1), 23–42.

Webley, L., 2010, 'Qualitative approaches to empirical legal research', in H.K. Peter Cane (ed.), *Oxford handbook of empirical legal research*, pp. 1–21, Oxford University Press, London.

White, H.D., 2007, 'Combining bibliometrics, information retrieval, and relevance theory, Part 2: Some implications for information science', *Journal of the Association for Information Science and Technology* 58(4), 583–605. https://doi.org/10.1002/asi.20542

Wylie, J.J., Bigrigg, M.W., Strunk, J.D., Ganger, G.R., Kiliccote, H. & Khosla, P.K., 2000, 'Survivable information storage systems', *Computer* 33(8), 61–68. https://doi.org/10.1109/2.863969

Yang, Z., Yang, M., Zhang, Y., Gu, G., Ning, P. & Wang, X.S., 2013, 'Appintent: Analyzing sensitive data transmission in android for privacy leakage detection', in A.R. Sadeghi, V. Gligor & M. Yung (eds.), *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, ACM, Berlin, Germany, 04–08 November, pp. 1043–1054.

Young, A.L. & Quan-Haase, A., 2013, 'Privacy protection strategies on Facebook: The Internet privacy paradox revisited', *Information, Communication & Society* 16(4), 479–500. https://doi.org/10.1080/1369118X.2013.777757