11th International Conference on Research in SCIENCE & TECHNOLOGY

14_16 May, 2021
Paris, France

RSTCONF

Challenges of implementation of data protection legislation in a South African context

Marvin Walter Theys, Prof. Ephias Ruhode and Dr. Patricia Harpur
Faculty of Informatics and Design Cape Peninsula University of Technology Cape Town, South Afric

Abstract.

South Africa has enacted its own information protection law, the Protection of Personal Information (POPI) Act, in 2013. 2018 saw the publication of the regulations. Neither the Act nor its regulations provide recommendations that assists organizations with achieving compliance. Furthermore, POPI impacts businesses from various sectors differently. The type of personal information stored and required for processing differs across organizations. Moreover, fines issued under the POPI Act could reach as high as 10 million Rand. This paper outlines a case study which explored within a single organization to identify what the challenges are that an organization could be faced with. The study is conducted throughout the organizational levels within a single organization. In the light of the imminent enforcement of the POPI Act, this paper highlights challenges that organizations could experience.

Keywords: POPI, Data protection South Africa, implementation, challenges, compliance

1 INTRODUCTION

Data protection is currently a hot topic from all corners of the globe (Wagner & Frank, 2018). South Africa has followed suite with the rest of the world and enacted the Protection of Personal Information (POPI) Act, signed into law by the South African President in November 2013 (Welz, 2016). POPI saw its first publication in the South African National Gazette during this time. In recent year she POPI Act gain some traction as the Information Regulator was officially appointed in 2016 (Burger-Smidt, 2016). The regulations of POPI were published in December 2018 (South African Government, 2013). A one-year grace period to comply with POPI, starting from the date that the act comes into full effect, will be granted to companies (Buys, 2018). Fines imposed for non-compliance could be as high as ten million Rand (South African Government, 2013).

The purpose of POPI is to ensure the security of personal or private information processed, by either a public or a private body, through:

- Establishing baseline requirements for secure processing or handling of personal or private information

- Appointing of an Information Regulator which deals with complaints and related matters
- Providing a basis for issuing codes that relate to conduct

- Including the basic rights of persons or individuals in terms of unwanted electronic communications
- Governing the cross-border movement of personal or private information in South Africa

It fails to make recommendations that assist with compliance.

The following sections will incorporate data protection laws from the European Union and Canada.

2 BACKGROUND

This section covers the following emergent themes:

- Technical Measures
- Consent
- Data Protection Officers.

2.1 Technical Measures

The General Data Protection Regulation (GDPR) of the European Union (EU) recommends the use of encryption as a method to protect data (GDPR, 2016). The Personal Information Protection and Electronic Document Act (PIPEDA) of Canada mentions encryption as well (Government of Canada, 2012). Encryption, which is also called encipherment, is the process of disguising information as "ciphertext," or rendering data unintelligible to an unauthorized person (Gregersen, Parul, & Lotha, 2017). The advanced encryption standard (AES) or Rijndael, an encryption scheme, permits decryption of encrypted data by using a secret key thus implying that AES provides secure data storage (Kocabas & Soyata, 2015). The United States National Institute of Standards and Technology (NIST) accepted the AES algorithm in 2001 (Naman, Bhattacharyya, & Saha, 2018). AES became a standard of the Federal Government (Naman et al., 2018). POPI does not mention encryption, it only requires reasonable technical measure be put in place to secure information. The Regulation of Interception and Communications Act (RICA) of South Africa also mentions decryption but does not mention specific methods (Government Gazette, 2003). Could AES encryption then be considered as reasonable technical measure?

2.2 Consent

The GDPR requires consent from individuals to have their information processed (GDPR, 2016). EU Regulation Section 33 states that it accepts both written and electronic methods for obtaining consent (GDPR, 2016). PIPEDA, in Section 4.3.2, states that consent from individuals for information processing is required (Government of Canada, 2012). Consent regulations impacted Canadian researchers negatively (Harris, Levy, & Teschke, 2008). It was also recommended that the consent regulation of PIPEDA be strengthened to remain on par with current technological advances (Trosow, Tremblay, & Weiss, 2016). POPI requires written consent for direct marketing purposes which will be monitored by the Information Regulator (Bruyn, 2014). POPI does not require consent if personal information collected is for a legal purpose (Burger-Smidt, 2016).

2.3 Data Protection Officers

GDPR requires a Data Protection Officer (DPO) where large volumes of data is being processed (GDPR, 2016). The DPO will handle compliance matters relating to GDPR within a specific organisation (Boban, 2016). DPO's are considered as crucial entities within organizations (Chassang, 2017). PIPEDA does not require a data protection officer as the Privacy Commissioner will deal with contraventions (C. Bennett, 2018). Canada also enacted a statute aimed specifically at the private sector (C. J. Bennett, Regan, & Bayley, 2017). POPI requires the designation of an Information Officer (IO) (Burger-Smidt, 2016). The IO will be the link between supervisory authorities, the organizations and the complainants.

The study reviews the following research question:

What are the challenges when implementing data protection legislation in South Africa?

3 METHOD

Since a case study allows the researcher the opportunity to investigate a phenomenon in a real-life setting and to collect rich and thick data (Yin, 1994), it was conducted within a single organisation. Organisations typically consists of three hierarchical levels namely: Strategic, Tactical and Operational (Anthony, 1965). Fig. 1. Shows the grouping of the respondents based on the level within the organisational hierarchy.

Figure 1: Organization Hierarchy with Interview Respondents

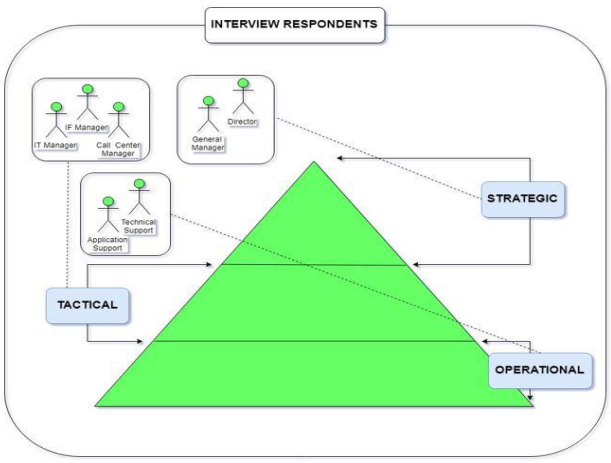


Figure 1 illustrates the strategic level comprises two respondents namely, the director and the general manager. The tactical level respondents are departmental managers and the operational level consists of call centre staff as well IT staff.

Data collection methods included interviews and survey questionnaires. Interview and survey questions were structured to suit relevant organizational levels of the respondents. Furthermore, the questions were informed by literature.

The data was collected throughout the organisational levels and subsequently analysed thematically. The questionnaires contained Likert Scale items. The options were presented to measure how strongly respondents agreed with the statement. The options were:

- Totally Agree
- Partially Agree
- Slightly Agree
- Totally Disagree.

Both the interview and survey respondents were assured of anonymity, confidentiality and the right to refuse. Furthermore, the nature of the study was communicated. In total, 3 respondents were interviewed, each representing an organizational level. The questionnaires were distributed throughout the organizational levels. The totals were as follows:

- Strategic – 1
- Tactical – 3
- Operational – 20

Interviews were recorded and transcribed. The transcriptions were then analysed thematically. Atlas.ti was used to assist with the grouping of themes. Questionnaires were analysed thematically as well.

To ensure that enough staff were available to meet daily operational goals, the respondents were grouped into small clusters. The clusters were then allocated specific times for them to participate in the survey. Interviews were scheduled differently as these were one on one sessions.

4 FINDINGS

This section focusses on the themes that have emerged during analysis. Findings will be presented, and a summary will close off the chapter.

4.1 Significance of backups

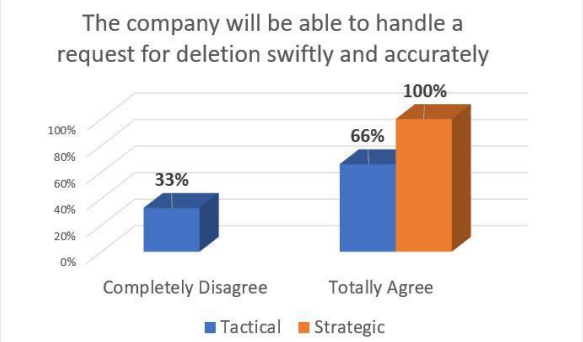
POPI guarantees the individual the right to request that their personal information be removed. In the event of a data processor not needing the stored information, it also should take steps to have such data removed. Even a technology company like *Google* got a request to remove an individual's information and was forced to facilitate this (Watanabe, 2017). The two strategies, backup and recovery, ensure the survival of a business (Nelson, 2011). In this case, the emails and data stored in an electronic database form part of the company's backup strategy.

In an interview with one respondent, the Information Technology Support Technician (ITST) from the operational level, it was stated that emails are backed up and that these backups go as far back as five years. He also stated that if a request to delete information that is backed up is received, it would be a resource-and effort-consuming activity.

According to the ITST, personal information that gets backed up gets done so on a weekly, monthly and yearly basis. Handling a request for deletion, taking into consideration the time that this data was stored, will mean revisiting and modifying multiple backups just to facilitate one person's request to have his or her data removed.

Conversely to the opinion of the ITST, respondents from the strategic and tactical organisation levels had a completely different view. The survey presented to these respondents were Likert scale and it contained the statement "The company will be able to handle a request for deletion swiftly and accurately". Fig. 2 is a graphical representation all responses.

Figure 2: The company will be able to handle a request for deletion swiftly and accurately



After analysis it was found that the Strategic (100%) level respondent and slightly more than half of the Tactical (66%) level were in full agreement with the statement. A small amount (33%) was in full disagreement with the statement. The operational staff were excluded from this statement as it was not in their respective questionnaire. Deletion of personal information can have a tremendous impact on businesses (Kampmark, 2015).

4.2 Outdated Methods

POPI requires written consent from an individual by an organisation for the use of his or her information for the purpose of direct marketing. The Administration Manager (AM), interview respondent from the Tactical operational level, stated that working with paper-based information is not practical. She also commented that faxing and printing does not "fit in this day and age". She then continued and stated that the business only sends electronic communications to clients as this is a practical way to do things. She closed off the response by saying that doing things via the Post Office in this century is considered ancient.

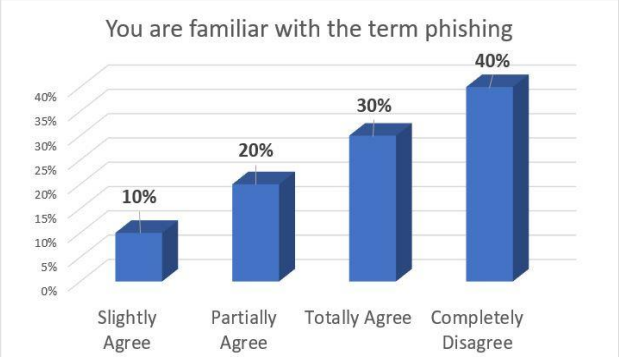
During an interview with the General Manager (GM) she stated that dealing with hard copies of information will be a massive challenge. She explained that the reason for the challenge is that information was stored in that manner before the company shifted to electronically managed data. Furthermore, she stated that even retrieving such information would be a very difficult task as the information was not necessarily stored according to a fixed filing system. So, in the event of the organisation receiving a request to remove or delete personal information stored in a warehouse as hard copies would be a very tough and could become a very expensive exercise.

4.3 Staff and Skills Training

It has been illustrated that irrespective of the level of technical security measures put in place at an organisation, careless and ignorant behaviour by staff could compromise it (Box & Pottas, 2014). In terms of security, the weakest link is which is often identified is the human factor (Bellekens et al., 2016). Therefore, the questionnaires presented to the Operational level staff contained statements to determine their understanding of certain computer security concepts.

Phishing is a very old and well-known form of cyber-attack during which the personal information of an individual is stolen via the internet with malicious intent (Milletary, 2005). The questionnaire presented to the Operational Level staff listed the statement "You are familiar with the term phishing" and were given Likert scale options for the responses. In Fig.3 below the results are illustrated.

Figure 3: You are familiar with the term phishing



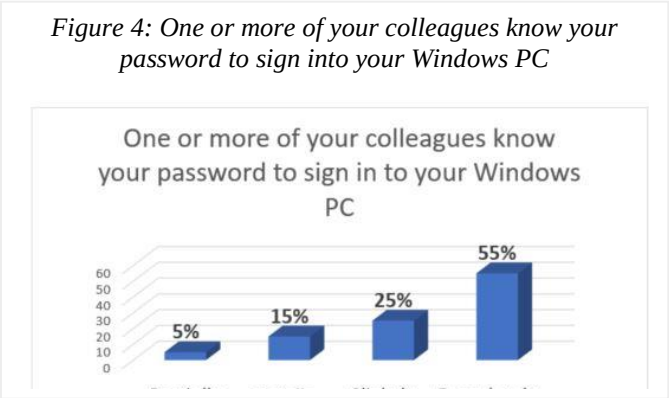
It turned out that slightly less than half (40%) completely disagreed with the statement with a smaller amount (30%) indicating that they totally agree These results indicate that only a hand full (30%) of operational staff are familiar with the term phishing, which is concerning.

The most powerful form of a cyber-attack is referred to as Social Engineering (Salahdine & Kaabouch, 2019). Social engineering is when the attacker or cyber-criminal attempts to guess what a user's password could possibly be. This achieved by researching the target or victim, creating a trusted relationship with the target, maliciously use the information gathered from the target, perform the illegal activity and then leave without a trace (Salahdine & Kaabouch, 2019). Social Engineering is also an alternative to attacking the technical measures put in place to

secure a system by simply going after the users themselves (Bansla, Kunwar, & Gupta, 2019). The questionnaire given to Operational Level staff contained the statement "One or more

of your colleagues know your password to sign into your Windows PC". Fig. 4. below show how the responses compare.

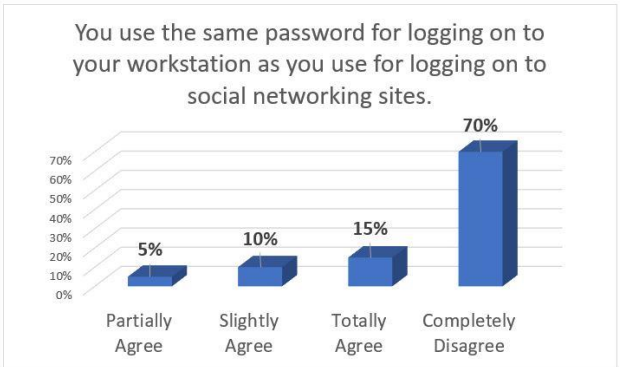
Figure 4: One or more of your colleagues know your password to sign into your Windows PC



It was reassuring to find that slightly more than half (55%) of respondents disagreed with that statement. It is concerning though that the rest of the respondents (45%) were either partially, slightly or in total agreement with the statement. Seeing that cyber-attacks are so dangerous, should keeping one's password private not be considered essential, not to mention common sense?

Another statement used in the questionnaire, following the premise of social engineering, "You use the same password for logging on to your workstation as you use for logging on to social networking sites" has yielded rather stable results. The results are shown in Fig. 5. below.

Figure 5: Statement regarding password usage



The majority (70%) of respondents completely disagreed with the statement. These results are indicative that the staff do have some understanding when it comes to password use but, there is still a gap (30%) that are not entirely informed. Therefore, staff training should be done regularly to keep them informed of latest developments in terms of computer security.

Across all operational levels, the questionnaires included the statement "You are aware of policies within your organisation that provides guidelines for ensuring that emails sent to clients are protected.". In Fig. 6 below, a decline is clearly visible.

Figure 6: Statement regarding policies

The results showed that there was a decline in policy knowledge based on the organisational level of the respondents. It started out with the strategic (100%) that agreed fully with the statement, second was the tactical level with most (66%) agreeing and then lastly few (35%) of the operational level staff provided the same answer. An interesting result in Fig. 6. shows a decline in security policy awareness as you move down the organizational hierarchy.

It is clear from the data presented that gaps do exist when it comes to staff awareness of cyber security and policies put in place to protect information. Another technology giant, Facebook, was forced to change their privacy law because of the GDPR and the Cambridge Analytica debacle (Shvartzshnaider, Apthorpe, Feamster, & Nissenbaum, 2018). Low awareness levels among staff constitute a risk and is therefore deemed a challenge when seeking full compliance to the POPI Act.

4.4 Cross Legislation Impact

Even though POPI grants the individual the right to have his or her personal information removed, there are separate legislations that compel companies to store personal information for a few years. One such legislation is the Financial Advisory and Intermediary Services (FAIS) Act of South Africa.

4.4.1 FAIS Act

The FAIS Act states that a financial institution should hold information for at least 5 years, this is mentioned in Chapter 5, Section 18 of the act (FAIS, 2002). During the open-ended interview with the GM she stated that POPI is in contradiction to what is required by the FAIS Act because POPI grants individuals the right to have their information removed. The GM commented further by adding that FAIS does not require any hard copies of information, soft copies are acceptable. The ITST also stated during the interview that he is aware that FAIS requires them to keep records for up to five years and this provides the basis for the backup strategy. It is therefore imperative that companies find out how exactly POPI impacts their businesses.

4.4.2 FICA Act

The Financial Intelligence Centre Act (FICA) of 2001 requires an attorney to report possible fraudulent activities and failure to do so might result in a fine(Burdette, 2010). Furthermore, also states that information is not privileged and the right to confidentiality can be limited by legislation (Burdette, 2010). Lastly, FICA requires records be kept for at least five years (Financial Intelligence Centre, 2017). POPI, on the other hand, grants individuals the right to have their information removed. The question is, if an individual request their information removed, right after committing a crime, would POPI allow it? During the interview with the AM, she mentioned that she does verification of ID Numbers by sending them to credit bureaus with the sole purpose of determining whether a client has a good or bad credit record. If clients could remove their information from the credit bureaus, would POPI allow individuals to cover their tracks?

5 DISCUSSION AND RECOMMENDATIONS

This study reviewed the challenges associated with the implementation of data protection legislation in a South African context. The following research question was posed:

What are the challenges when implementing data protection legislation in South Africa?

Below is a list of challenges as well as possible remedial actions.

5.1 Dealing with backups

When removing personal information, consideration should be given to deletion protocols and data stored in backups.
Old information might re-surface when backups are restored. Therefore, processes should be put in place
that will prevent the restoration of data that has been previously deleted.

5.2 Hard copy or paper-based information

Organizations will face challenges when dealing with hard copies of personal information. All personal information should be stored in a way that makes it easily retrievable, verifiable and removeable. All hard copies should be scanned, and then discarded. Organizations should, where applicable, gather all hard copies and convert to electronic documents. Neither POPI nor its regulations offer a remedy for this.

5.3 Staff Training

Employees are the easiest targets for hackers. Organizations should invest in workshops for staff aimed at educating and empowering staff with the most up to date information on hacking techniques. Frequent assessments should be done in addition to this as an additional safeguard.

5.4 Cross Legislation Impact

Organizations should begin assessments on the different laws that impact the organization. POPI does not make
mention of when this occurs. Furthermore, it does not provide remedies either. POPI has a bespoke impact on organizations. Therefore, cross legislation impact should be investigated.

6 Conclusions and Future Research

This study highlighted four major challenges, including:

- Significance of backups;
- Outdated methods linked to hard copy or paper-based information;
- A need for staff training; and
- Consideration of cross-legislation impact.

Organisations should start preparing for when POPI does come into full effect. POPI will impact various businesses and organisations differently and it should be considered, as a top priority, to start planning the implementation of POPI's requirements. At the time of writing this article, POPI was not yet in full effect. As soon as this happens, a 12-month grace period will be granted. To ensure compliance in organisations, it is therefore imperative that the development of deletion protocols is commenced as soon as possible.

This paper contributes theoretically, practically and methodologically to the implementation of data protection legislation.

Future research plans to address a real-world implementation.

7 References

Anthony, R. N. (1965). *Planning and Control: a Framework for Analysis*. Cambridge MA: Harvard University Press.

Bansla, N., Kunwar, S., & Gupta, K. (2019). Social Engineering : A Technique for Managing Human Behavior. *Social Engineering: A Technique for Managing Human Behavior*, *5*(1), 18–22. https://doi.org/10.5281/zenodo.2580822

Bellekens, X., Nieradzinska, K., Bellekens, A., Seeam, P., Hamilton, A., & Seeam, A. (2016). A Study on Situational Awareness Security and Privacy of Wearable Health Monitoring Devices. *International Journal on Cyber Situational Awareness*, *1*(1), 74–96. https://doi.org/10.22619/ijcsa.2016.100104

Bennett, C. (2018, April 12). *Data Driven Elections and Political Parties in Canada: Privacy Implications, Privacy Policies and Privacy Obligations*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3146964

Bennett, C. J., Regan, P. M., & Bayley, R. M. (2017). If these Canadians lived in the United States, how would they protect their privacy? *First Monday*, *13*, 98–107.

Boban, M. (2016). Digital Single Market and Eu Data Protection Reform With Regard To the Processing of Personal Data As the Challenge of the Modern World. *Economic and Social Development (Esd)*, (September), 191–201.

Box, D., & Pottas, D. (2014). Improving Information Security Behaviour in the Healthcare Context. *Procedia Technology*, *9*, 1093–1103. https://doi.org/10.1016/j.protcy.2013.12.122

Bruyn, M. De. (2014). *The Protection Of Personal Information (POPI) Act - Impact On South Africa*. *13*(6), 1315–1340.

Burdette, M. (2010). *IS THE REPORTING OBLIGATION OF ATTORNEYS IN TERMS OF SECTION 29 OF THE FINANCIAL INTELLIGENCE CENTRE ACT 38 OF 2001 A MYTH OR A REALITY ?*

Burger-Smidt, A. (2016). Appointment of Information Regulator - Werksmans | Werksmans Attorneys. Retrieved February 24, 2019, from https://www.werksmans.com/legal-updates-and-opinions/appointment-of-information-regulator-2/

Buys, M. (2018). Protecting personal information: Implications of the Protection of Personal Information (POPI) Act for healthcare professionals. *South African Medical Journal*, *107*(11), 954. https://doi.org/10.7196/samj.2017.v107i11.12542

Chassang, G. (2017). The impact of the EU general data protection regulation on scientific research. *Ecancermedicalscience*, *11*, 709. https://doi.org/10.3332/ecancer.2017.709

FAIS. (2002). *Financial Advisory and Intermediary Services Act*. *449*(37). Retrieved from http://www.info.gov.za/view/DownloadFileAction?id=68072

Financial Intelligence Centre. (2017). *FINANCIAL INTELLIGENCE CENTRE ACT, 2001 (Act No. 38 OF 2001)*. *2001*(38), 1–75. Retrieved from https://www.fic.gov.za/Documents/FIC Act with 2017 amendments (1) (1).pdf

GDPR. (2016). *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016*. *2014*(April), 143. https://doi.org/http://eur-lex.europa.eu/pri/en/oj/dat/2003/l_285/l_28520031101en00330037.pdf

Government Gazette. (2003). Act No. 70,2002 REGULATION OF INTERCEPTION OF COMMUNICATIONSe AND PROVISION OF COMhlUNICATIOK-RELATED INFORMATION ACT. 2002. *Government Gazette*, *451*(70), 1–49.

Government of Canada. (2012). Personal Information Protection and Electronic Documents Act Loi sur la protection des renseignements personnels et les documents électroniques. *ReVision*. https://doi.org/10.1080/01431160903475274

Gregersen, E., Parul, J., & Lotha, G. (2017). Data encryption | cryptology | Britannica.com. In *Britannica*. Retrieved from https://www.britannica.com/technology/data-encryption

Harris, M. A., Levy, A. R., & Teschke, K. E. (2008). Personal privacy and public health: Potential impacts of privacy legislation on health research in Canada. *Canadian Journal of Public Health*, *99*(4), 293–296.

Kampmark, B. (2015). To Find or be Forgotten: Global Tensions on the Right to Erasure and Internet Governance. *Journal of Global Faultlines*, *2*(2), 1. https://doi.org/10.13169/jglobfaul.2.2.0001

Kocabas, O., & Soyata, T. (2015). Towards privacy-preserving medical cloud computing using homomorphic encryption. *Enabling Real-Time Mobile Cloud Computing through Emerging Technologies*, 213–246. https://doi.org/10.4018/978-1-4666-8662-5.ch007

Milletary, J. (2005). Technical Trends in Phishing Attacks. *Technical Trends in Phishing*, 1–17. Retrieved from https://resources.sei.cmu.edu/asset_files/WhitePaper/2005_019_001_50315.pdf

Naman, S., Bhattacharyya, S., & Saha, T. (2018). Remote Sensing and Advanced Encryption Standard Using 256-Bit Key. *Advances in Intelligent Systems and Computing*, *937*, 181–190. https://doi.org/10.1007/978-981-13-7403-6_11

Nelson, S. (2011). *Pro Data Backup and Recovery* (1st Editio). Apress.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4). https://doi.org/10.3390/FI11040089

Shvartzshnaider, Y., Apthorpe, N., Feamster, N., & Nissenbaum, H. (2018). *Analyzing Privacy Policies Using Contextual Integrity Annotations*. 1–18. https://doi.org/10.1093/forestscience/46.1.116

South African Government. (2013). *Protection of Personal Information Act, 2013 Ensuring protection of your personal information and effective access to information*. (4), 154. https://doi.org/10.1006/brcg.1998.0994

Trosow, S. E., Tremblay, S., & Weiss, D. (2016). Consultation on Consent and Privacy.

Wagner, L., & Frank, R. (2018). *Understanding the Importance of FERPA & Data Protection in Higher Education . An Application : Website at La Salle University Understanding the Importance of FERPA & Data Protection in Higher Education . An Application : Website at La Salle*.

Watanabe, P. J. (2017). *AN OCEAN APART : THE TRANSATLANTIC DATA PRIVACY*.

Welz. (2016). A SUMMARY OF "POPI" THE PROTECTION OF PERSONAL INFORMATION ACT, ACT No. 4 OF 2013 | Miltons Matsemela. Retrieved February 24, 2019, from https://www.miltons.law.za/a-summary-of-popi-the-protection-of-personal-information-act-act-no-4-of-2013/

Yin, R. K. (1994). *Case study research: design and methods*.