Cyber Security, Cyber Crime and the Protection of Personal Information (Data Protection) –

2nd Africa Cyber Crime Forum

Organized by COE and AU

Prof Sizwe Lindelo SNAIL ka Mtuze

Adjunct Professor Nelson Mandela University

Member – Information Regulator South Afri

Director Snail Attorneys @ Law

NELSON MANDELA UNIVERSITY

- The Regulator derives its Constitutional mandate from sections 14 (The right to privacy)

  and 32 (The right of access to information) ito the Constitution of RSA, 1996.
- Section 40 of POPIA makes provision for the powers, duties and functions of the Regulator.
- Sections 2 to 38; sections 55 to 109; section 111; and section 114 (1), (2) and (3)

  commenced on 1 July 2020.
- Sections 110 and 114(4) shall commence on 30 June 2021.
- The PAIA function still remains with the South African Human Rights Commission (SAHRC) and will be transferred to the Regulator in terms of section 114 (4) of POPIA on the 30 June 2021

NELSON MANDELA UNIVERSITY

Who are the Role Players?

ROLE PLAYER	FUNCTION
Data Subject	Person to whom information relates
Responsible Party	A public or private body or any other person which alone or in conjunction with others determines the purpose of and means for processing personal information.
Operator	A person who processes personal information for a responsible party in terms of a contract or mandate without coming under the direct authority of that party.
Competent Person	Any person who is legally competent to consent to any action or decision being taken in respect of a matter concerning a child

NELSON MANDELA UNIVERSITY

Definitions: What is Personal Information?

Personal information is information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

(b) information relating to the education or the medical, financial, criminal or employment history of the person;

NELSON MANDELA UNIVERSITY

Rights of A Data Subject

The rights of a data subject are clearly set out in section 5 and are largely the consequences of the broader right to privacy. In terms of section 5 a data subject has the right to have his, her or its personal information processed in accordance with the conditions for the lawful processing of personal information as referred to in Chapter 3 of POPIA.

- Section 5 (a) (i) and (ii) provide that a data subject has the right to be notified that personal information about him, her or it is being collected as well as the right to know when his or her or its personal information has been accessed or acquired by an unauthorized person as provided for in terms of sections 18 and 23.
- Section 5 (b) goes further in affording the data subject the right to establish whether a responsible party holds personal information of that data subject and to request the responsible party access to his, her or its personal information as provided for in terms of section 23.
- Section 5 (c) and (d) guarantee the data subject the right to request, where necessary, the correction, destruction or deletion of his, her or its personal information as provided for in terms of section 24 and also confer upon a data subject the right to object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its personal information as provided for in terms of section 11(3)(a).

Rights of A Data Subject cont.

- In addition a data subject has the right to object to the processing of his, her or its personal information at any time for purposes of direct marketing, in terms of section 11(3)(b) or, alternatively, in terms of section 69(3)(c). The latter section provides that a data subject has the right to object to having his, her or its personal information processed for purposes of direct marketing by means of unsolicited electronic communications, except as referred to in section 69(1) as provided for by section 5 (e) and (f).
- Furthermore, a data subject has the right not to be subject, under certain circumstances, to any decision which is based solely on the basis of the automated processing of his, her or its personal information intended to provide a profile of such person as provided for in terms of section 71 and 5 (g).
- Lastly, a data subject has the right to submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of any data subject, or to submit a complaint to the Regulator in respect of a determination of an adjudicator as provided in terms of Section 74. Moreover, a data subject may institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information as provided for in Sections 9, and section 5 (h) and (i).

8 (eight) Conditions for Lawful Processing of Personal Information

- The POPIA has brought into law new duties on processors of personal information to safeguard personal information and to ensure that processing complies with the 8 (eight) Conditions for lawful processing of personal information.

- In terms of Section 4 there are 8 (eight) Conditions for lawful processing of personal information.

- These conditions, found in sections 8 to 25 of the POPIA which is the supreme piece of legislation dealing with Data Protection, are the following: (a) accountability (section 8); (b) processing limitation (sections 9 to 12); (c) purpose specification (sections 13 and 14); (d) further processing limitation (section 15); (e) information quality (section 16); (f) openness (section 17 and 18); (g) security safeguards (section 19 to 22); and (h) data subject participation (section 23 to 25).

The 1 (One) year Grace Period

- It is not period to continue non-compliance with POPIA by a Responsible

- The Grace Period is a period for Responsible parties to get compliant with the POPIA

- Responsible parties are encouraged to proactively comply and will be assisted by the Regulator to identify and remedy data protection compliance issue

NELSON MANDELA UNIVERSITY

Definitions: What is Special Personal Information?

In terms of Section 26 of POPIA Special Personal Information is:

(a)the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or

(b)the criminal behaviour of a data subject to the extent that such information relates to

(i) the alleged commission by a data subject of any offence; or
(ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

What is Processing?

“Processing’’ means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including-

(a)the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

(b)dissemination by means of transmission, distribution or making available in any other form; or

(c)merging, linking, as well as restriction, degradation, erasure or destruction of information.

What is Processing?

Processing may only take place where the data subject consents to the processing, processing is necessary in certain contractual situations, in terms of a legal obligation or the proper performance of a public law duty, processing is necessary to uphold a legitimate interest of the data subject, necessary to pursue the legitimate interest of a responsible person.

NELSON MANDELA
UNIVERSITY

- The POPIA is not aimed at preventing and / or stopping all processing of personal information, but rather seeks to manage and enable ethical processing, as well as the use of personal information within the context of our constitutionally driven society. In another landmark case of *Black Sash Trust v Minister of Social Development* 2017(3) SA 335 (CC) the Constitutional court held:

- *"SASSA is under a duty to ensure that the payment method it determines … contains adequate safeguards to ensure that personal data obtained in the payment process remains private and may not be used for any purpose other than payment of the grants or any other purpose sanctioned by the Minister … precludes a contracting party from inviting beneficiaries to "opt in" to the sharing of confidential information for the marketing of goods and services."*

NELSON MANDELA UNIVERSITY

Eight Conditions of Lawful Processing

Condition	
Condition 1 Accountability	Responsible party must ensure compliance with the conditions for lawful processing.
Condition 2 Processing Limitation	PI must be processed lawfully, in a reasonable manner that does not infringe the privacy of the data subject. Minimality- adequate, relevant and not excessive. Consent, justification and objection; Collection directly from data subject

NELSON MANDELA UNIVERSITY

Eight Conditions of Lawful Processing

Condition	
Condition 3 Purpose Specification	PI must be processed lawfully, in a reasonable manner that does not infringe the privacy of the data subject. Minimality- adequate, relevant and not excessive. Consent, justification and objection; Collection directly from data subject
Condition 4 Further Processing Limitation	Further processing must be compatible with the purpose of collection failing which consent must be obtained, further processing is necessary for the maintenance of the law, comply with an obligation imposed by law, conduct of court proceedings, in the interests of national security, prevent or mitigate a serious and imminent threat historical, research, statistical purposes

Eight Conditions of Lawful Processing

Condition	
Condition 5 Information Quality	Personal information must be complete, accurate, not misleading and updated.
Condition 6 Openness	Responsible party must maintain records, Notification to data subject when collecting personal information

Eight Conditions of Lawful Processing

Condition	
Condition 7 Security Safeguards	A responsible party must secure the integrity and confidentiality of personal information. Information processed by an operator or person acting under authority must be done with the knowledge/authority of the responsible party. Information must be treated as confidential Security measures must adhere to security measures and notify the responsible party immediately if there is a breach.
Condition 8 Data Subject Participation	Data Subject must have access to PI. Correction or deletion of PI if inaccurate, irrelevant outdated, excessive, incomplete, misleading or unlawfully obtained.

NELSON MANDELA UNIVERSITY

Exemptions

The Regulator may exempt processing of personal information if satisfied that it is in the public interest and involves a clear benefit to the data subject or third party and outweighs any interference to privacy.

Public interest includes:

a) interests of national security
b) Prevention, detection and prosecution of offences
c) Important economic and financial interests of a public body
d) Fostering compliance with legal provisions
e) Historical, statistical or research activities
f) The special important of the interest in freedom of expression

NELSON MANDELA UNIVERSITY

Exemptions

Personal information processed for the purpose of discharging a Relevant function (of a public body, conferred on any person ito the law)

Consent

Section 11 Personal Information may only be processed with the consent of a data subject or consent of a competent person in relation to children Consent is any voluntary specific and informed expression of will in terms of which permission is given for the processing of personal information.

NELSON MANDELA UNIVERSITY

SECURITY SAFEGUARDS

- Condition seven (7) of the eight (8) conditions for processing of personal information stipulates the security measures that the responsible party must put in place to ensure the integrity and confidentiality of personal information in its possession.

- These measures are provided for in sections 19 to 22 of POPIA.

- These security safeguards, if properly applied will contribute to the prevention of data leaks, which South Africa is currently experiencing.

NELSON MANDELA UNIVERSITY

SECURITY SAFEGUARDS (cont.)

- The Cybercrimes Bill once it becomes law will also deal decisively with cybercrime.
  - What are the obligations of a responsible party regarding security safeguards (section 19 – 22 of POPIA)
- The responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking reasonable technical and organisational measures to prevent-
  - loss of, damage to or unauthorised destruction of personal information; and
  - Unlawful access to or processing of personal information.

NELSON MANDELA UNIVERSITY

SECURITY SAFEGUARDS (cont.)

- This in essence requires the responsible party to not only ensure the physical security of personal information in its possession, but also to ensure that the confidentiality of such information is secured.
- The responsible party must also actively familiarise itself with the security practices and procedure applicable to its industry and assess the efficacy of its security measures on an ongoing basis.
- The responsible party. For example, it provides that the controller and processor must implement appropriate technical and organisational measurers to ensure a level or security and confidentiality of data.

NELSON MANDELA UNIVERSITY

SECURITY SAFEGUARDS (cont.)

- Section 19 (2) of POPIA provides that in order to give effect to section 19(1), the responsible party must take reasonable measures to:

  (a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

  (b) establish and maintain appropriate safeguards against the risks identified;

  (c) regularly verify that the safeguards are effectively implemented; and

  (d)ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

- The responsible party remains accountable for the processing of personal information by its representative or operator. Hence section of POPIA provides that an operator or any one processing personal information on behalf of an operator must:

NELSON MANDELA UNIVERSITY

SECURITY SAFEGUARDS (cont.)

- process such information only with the knowledge or authorisation of the responsible party; and
- treat personal information which comes to their knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties.

- Responsibilities of a Operator
- Section 21 of POPIA provides as follows:
  - A responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator which processes personal information for the responsible party establishes and maintains the security measures referred to in section 19.
  - The operator must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

NELSON MANDELA UNIVERSITY

SECURITY SAFEGUARDS (cont.)

- Section 22 of POPIA provides that where the responsible party has reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by unauthorised person, the responsible party must notify:
  - the Regulator and
  - the data subject, unless the identity of such data subject cannot be established
  - The notification referred to in subsection (1) must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

NELSON MANDELA UNIVERSITY

SECURITY SAFEGUARDS (cont.)

-The responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

- The manner of notification

- The notification to a data subject referred to in subsection (1) must be in writing and communicated to the data subject in at least one of the following ways:

(a) Mailed to the data subject's last known physical or postal address;

(b) sent by e-mail to the data subject's last known e-mail address;

(c) placed in a prominent position on the website of the responsible party;

(d) published in the news media; or

(e) as may be directed by the Regulator.

NELSON MANDELA UNIVERSITY

SECURITY SAFEGUARDS (cont.)

- The notification referred to in subsection (1) must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including—

  (a) a description of the possible consequences of the security compromise;

  (b) a description of the measures that the responsible party intends to take or has taken to address the security compromise;

  (c) a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and

  (d) if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

- The Regulator may direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

NELSON MANDELA UNIVERSITY

- In the South African context, the importance of observing organizational and technical measures as required by the POPIA can never be overstated considering that during the course of August 2020, the entity known as ‘Experian’, which is a consumer, business and credit information service agency experienced a data breach.

- Other well publicized Data Breach include the email hack on Liberty Insurance where confirmation was given that the personal information of its Clients had been breached; the ViewFines Data Breach where the driving licenses of about 943 000 (Nine hundred and forty three thousand) road users whose names, personal identity numbers and email addresses in plain text on the ViewFines website were breached; the Data Breach at the offices of the Master of the High Court and the Deeds Registrar where varied personal information is held was breached;

- The hacking of the database of Ster-Kinekor in 2017, which contained names an email addresses of members of the public that use the movie house.

Data Protection Law meets Cyber Crime Legislation

- Within the context of Data Protection and Cyber Security, the legislature has demonstrated its acknowledgement of South Africa's transition in the 4IR by putting into force , subject to a grace period , the remaining Sections of the Protection of Personal Information Act No. 4 of 2013 (the 'POPIA') on the 1st July 2020 as well as the Cyber Crime Bill whose purpose entailed the protection of computer systems, the provision of criminal sanction in the event of Cyber Crimes

- The POPIA makes it obligatory to comply with the conditions for lawful processing of personal information, but also places an obligation on responsible parties to disclose breaches of information, provide data subjects with remedies where the POPIA makes provision for same and give the Information Regulator (hereafter the Regulator) power to impose severe penalties for such conduct.

NELSON MANDELA UNIVERSITY

- The advent of the 4IR brings about rapid digital technology advancements which have become fertile ground for various cyber-attacks and offences such as cyber fraud, extortion, as well as forgery; malicious damage to property in the form of computer viruses; child pornography; hacking; cracking; and various other online activities.

- The occurrence of various Cyber Crime becoming a commonplace phenomenon is the reason that the legislature deemed it fit to make provision (Chapter XIII) in the Electronic Communication and Transactions Act (ECTA) for the regulation of unauthorized access to, interception of or interference with data; computer-related extortion, fraud and forgery; attempt at aiding and abetting; and it set out the penalties for persons convicted in relation to particular provisions of the ECTA.

- The provisions in the ECTA relating to Cyber Crime are accordingly amended by those contained in the Cyber Crime Act. Act 19 of 2021.

- The State President signed into the Law the Cyber Crime Act on the 1 June 2021 – the Commencement date to be determined at a later date.

- The Cyber Crime Act has 3 (two) substantive criminal law parts –

- Part 1 – CYBER-CRIMES against Confidentiality, Availability , Data, Data Systems, Computer Systems

- Part 2 – Cyber Related Offenses and

- Part 3-Agrrevated (MALICIOUS COMMUNICATIO),

NELSON MANDELA UNIVERSITY

- The preamble of the Cyber Crime Act , Act 19 of 2021 states that its purpose among other things is to create offences which has a bearing on Cyber Crime and to prescribe penalties for such crimes.” For purposes of this article only the provisions on section 2 and 3 relation to Cyber Crime and Cyber Security.
- Section 2 of the Act makes provision for the unlawful securing of access. This section regulates that any person who unlawfully and intentionally secures access to data, a computer programmer, a computer data storage medium or, a computer system is guilty of an offence. Section 3 of the Act regulates the unlawful acquiring of data.
- Section 4 of the Act, Any person who unlawfully and intentionally overcome any protection measure which is intended to prevent access to data and acquires data, within or which is transmitted to or form a computer system is guilty of an offence the Cyber Crimes Act, Act 19 0f 2021

NELSON MANDELA
UNIVERSITY

- Section 5 of the Cyber Crimes Act makes the unlawfully and intentionally interferes with— (a) data; or (b) a computer program, is guilty of an offence. (2) For purposes of this section ‘‘interfere with data or a computer program
- Section 6 of the Cyber Crimes Act makes it unlawful for any person who unlawfully and intentionally interfere with a computer data storage medium or a computer system,
- For purposes of this section ‘‘interfere with a computer data storage medium or a computer system’’ means to permanently or temporarily— (a) alter any resource; or (b) interrupt or impair— (i) the functioning; (ii) the confidentiality; (iii) the integrity; or (iv) the availability, of a computer data storage medium or a computer system. Unlawful acquisition, possession, provision, receipt or use of password, access code or similar data or device
- Section 7 of the Cyber Crimes Act futher makes it criminal for any person who unlawfully and intentionally— (a) acquires; (b) possesses; (c) provides to another person; or (d) uses, a password, an access code or similar data or device for purposes of contravening

NELSON MANDELA
UNIVERSITY

- Cyber fraud, Cyber forgery and uttering as well as Cyber extortion have like wisely been criminalised by Section 8 , 9 and Section 10. of the Cyber Crimes Act
- Section 11 has now introduced Aggravated Offences by anyone any person who commits an offence referred to in— (i) section 3(1), 5(1) or 6(1), in respect of; or (ii) section 7(1), in so far as the passwords, access codes or similar data and devices relate to, a restricted computer system, is guilty of an aggravated offence. (b) For purposes of paragraph (a), a ‘‘restricted computer system’’ means any data, computer program, computer data storage medium or computer system— (i) under the control of, or exclusively used by— (aa) a financial institution; or (bb) an organ of state as set out in section 239 of the Constitution, including a court; and (ii) which is protected by security measures against unauthorised access or use.

- Section 14 specifically provides that any person who discloses, by means of an electronic communications service, a data message to a person, group of persons or the general public with the intention to incite a number of unlawful violations such as damaging property that belongs to a person or group of persons. It is important to note that inciting violence against a person or group of persons is encompassed in this provision. It is also unlawful to send a data message which threatens persons with damage to property or violence.

- Section 15 outlaws the use of an electronic communications service to unlawfully and intentionally disclose a data message which threatens a person with damage to property belonging to that person or a related person; or violence against that person or a related person.
- Furthermore, it is unlawful to send a data message that threatens a group of persons or any person forming part of, or associated with, that group of persons with damage to property belonging to that group of persons or any person

NELSON MANDELA UNIVERSITY

- With revenge pornography becoming commonplace, it is important to note the provisions set out in section 16. The Act provides at section 16(1) that any person who unlawfully and intentionally discloses (by means of an electronic communications service) a data message of an intimate image of a person without such a person's consent is guilty of an offence.

- In terms of section 2*(b)* the image may be real or simulated, and made by any means in which the person is nude, or the genital organs or their anal region is displayed. The Act specifies that where the person whose image is used is a female person, genital or anal region transgender person or intersex person. The sexual exploitation threshold is passed where a female person's breasts, whether covered or uncovered are displayed. The test laid out in sections 2*(b)(ii)(aa) – (bb*) is that the person whose image is used retains a reasonable expectation of privacy at the time that the data message was made in a manner that violates or offends the sexual integrity or dignity of the person*;* or amounts to sexual exploitation.

- Section 17*(a)* – *(c)* provides that any person who unlawfully and intentionally attempts, conspires with any other person, or aids, abets, induces, incites, instigates, instructs, commands or procures another person, to commit an offence set out in terms of Part I or Part II of Chapter 2 of the Act is guilty of an offence and is liable on conviction to the punishment to which a person convicted of actually committing that offence would be liable. Section 18 deals with *competent verdicts*.
- Section 18(1) provides that if the evidence in criminal proceedings does not prove the commission of an offence that is charged but proves a contravention of section 17*(a)* in respect of the offence charged, or in respect of any other offence of which an accused may be convicted on the offence charged, the accused may be found guilty if the offence is proved.

- The next important part of criminal proceedings in the context of cybercrimes is the aspect of sentencing. Section 19(1) provides that a contravention of sections 2(1) or (2), 3(3) or 7(2) renders a person liable on conviction to a fine or to imprisonment for a period not exceeding 5 (five) years, or to both a fine and such imprisonment. Section 19(2) provides that any person who contravenes the provisions of sections 3(1) or (2), 4(1), 5(1), 6(1) or 7(1) is liable on conviction to a fine or to imprisonment for a period not exceeding 10 (ten) years or to both a fine and such imprisonment. Section 19(3) provides that any person who contravenes the provisions of section 11(1) is liable on conviction to a fine or to imprisonment for a period not exceeding 15 (fifteen) years or to both a fine and such imprisonment.
- Section 19(4) provides that where the court convicts a person of an offence in terms of sections 8, 9(1) or (2), 10 or 11(2), it may (where a penalty is not prescribed in respect of that offence by any other law) impose a sentence (as provided for in section 276 of the Criminal Procedure Act, 1977) which that court considers appropriate and which is within that court's penal jurisdiction. Section 19(5) provides that where a court imposes any sentence in terms of this Section, or where a person is convicted of the offence of theft that was committed or facilitated by electronic means, it must do so having taken certain factors into consideration. The list of factors to be considered include the following, as set out in section 19(5)*(a) – (d):*

  (a) the fact that the offence was committed by electronic means;

  (b) the extent of the prejudice and loss suffered by the complainant or any other person as a result of the commission of such an offence;

  (c) the extent to which the person gained financially, or received any favour, benefit, reward, compensation or any other advantage from the commission of the offence; or

  (d) the fact that the offence was committed in concert with one or more persons.

- Section 19(6)*(a)* provides that if a person is convicted of any offence provided for in sections 2(1) or (2); 3(1); 5(1); 6(1); 7(1); 8; 9(1) or (2), 10 or 11(1) or (2), a court imposing any sentence in terms of those sections must impose a period of direct imprisonment, with or without a fine, if the offence was committed by the person; or with the collusion or assistance of another person, who as part of their duties, functions or lawful authority were in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system belonging to another person in respect of which the offence in question was committed.

- The exception to this rule is that the court should take this route unless substantial and compelling circumstances justify the imposition of another sentence. Section 19(7) provides that any person who contravenes the provisions of sections 14, 15 or 16 is liable on conviction to a fine or to imprisonment for a period not exceeding 3 (three) years or to both a fine and such imprisonment. Section 20(1) provides that a complainant who lays a charge with the South African Police Service (SAPS) that an offence contemplated in Section 14, 15 or 16 has allegedly been committed against them, may on an *ex parte* basis apply to a Magistrate's Court for a protection order pending the finalisation of the criminal proceedings.

- Such an application may be made to prohibit any person from disclosing or further disclosing the data message which relates to the charge; or order an electronic communications service provider whose electronic communications service is used to host or disclose the data message which relates to the charge, to remove or disable access to the data message. Section 20(2) provides that in determining such an Application, the court *must* consider any additional evidence it deems fit, including oral evidence or evidence by affidavit, which must form part of the record of the proceedings.

- In accordance with section 20(3), if the court is satisfied that there is *prima facie* evidence that an offence referred to in section 14, 15 or 16, has allegedly been committed against the applicant; and indeed there exist reasonable grounds to believe that a person referred to in subsection (1)*(a)* disclosed the data message in question, the court may, subject to such conditions as it may deem fit, issue the order referred to in subsection (1). The Act has effectively repealed all the relevant provisions in the ECT Act relating to cybercrime offences. It will consolidate and systemise numerous existing offences relating to cybercrime while also creating a variety of new offences which do not currently exist in the South African law. The Act also creates structures such as a 24/7 point of contact to report, investigate and prosecute any cybercrime related offences the 24/7 point of contact will operate on a 24 hour, 7 days a week basis.

NELSON MANDELA
UNIVERSITY

Conclusion

- In the South African context therefore it is clear that the intersection between Cyber Crime and Data Protection lies in that the POPIA calls for Security Safeguards
- The observation of organizational and technical measures in protecting personal information with financial / cost implications imposed by the Information Regulator on responsible parties in the event that they fail to observe the provisions of the POPIA
- The Cybercrimes Act sets out the penal implications for criminals against whose efforts and activities such technical and organizational measures are put in place.

NELSON MANDELA UNIVERSITY

Q & A

NELSON MANDELA UNIVERSITY

Contact :

Prof Sizwe Lindelo Snail ka Mtuze

E-mail : ssnail@Snailattorneys.com/
www : www.snailattorneys.com
Tel / Fax : + 27 (012) 7578761
Fax : + 27 (086) 617 5721
Cell : + 27 (083) 477 4377 (WhatsApp call and Video Call)

NELSON MANDELA
UNIVERSITY