ISPA
Internet Service Providers Association

CYBERCRIME AND THE LAW

Internet Service Providers Association

INTERNATIONAL LAW

Convention on Cybercrime / Budapest Convention

- first international treaty seeking to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations

  "pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation"
- Into force 1 July 2004
- 46 states ratified + 8 further signatories (including SA on 23 July 2001)
- Drawn up by the Council of Europe with the active participation of South Africa

Internet Service Providers Association

CYBERCRIME CONVENTION

Ratified / signed (into force)	Not ratified / signed
South Africa (n/a)	Brazil
United Kingdom (1 Sept 2011)	Russia
USA (1 Jan 2007)	India
Canada (1 Nov 2015)	China
Sri Lanka (1 Sept 2015)	

CYBERCRIME CONVENTION

- **Additional Protocol to the Convention on Cybercrime**
  - into force on 1 March 2006
  - requires criminalisation of dissemination of racist and xenophobic material + threats and insults motivated by racism/xenophobia through computer systems
- **Offences**
  - illegal access
  - illegal interception
  - data interference
  - system interference
  - misuse of devices
  - computer-related forgery
  - computer-related fraud
  - offences related to child pornography
  - and offences related to copyright and neighbouring rights.

CYBERCRIME CONVENTION

- Procedural law issues
  - expedited preservation of stored data
  - expedited preservation and partial disclosure of traffic data
  - production order, search and seizure of computer data
  - real-time collection of traffic data, and
  - interception of content data.
- International mechanisms
  - transborder access to stored computer data which does not require mutual assistance (with consent or where publicly available)
  - setting up of a 24/7 network for ensuring speedy assistance amongst parties

- **AU Convention on Cyber Security and Personal Data Protection**
  - adopted by AU on 27 June 2014
  - addresses a wide range of online activities, including electronic commerce, data protection, cybersecurity and cybercrime
  - Cybercrime: states must adopt laws that criminalise
    - Attacks on computer systems
    - Computerised data breaches
    - Content-related offences
    - Offences relating to electronic message security measures
  - Emphasis on capacity building, international cooperation and harmonisation of laws

Internet Service Providers Association

SOUTH AFRICA

SOUTH AFRICAN LAW

- **Electronic Communications and Transactions Act 2002**
  - Chapter 13 offences
- **RICA 2002**
  - Procedural provisions of Cybercrime Convention
- **Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007**
  - Child pornography
- **Film and Publications Act 1996**
  - Child pornography
- **Common law**
- **National Cybersecurity Framework May 2012 (not in public domain)**
- **Cybercrimes and Cybersecurity Bill**

Internet Service Providers Association

CYBERCRIMES & CYBERSECURITY BILL

- DOJCD mandated to review the cyber security laws to ensure they provide for a coherent and integrated cyber security legal framework
- Indication that in future may address cryptography, e-identity management and electronic evidence
- Alignment with Cybercrime Convention
- New institutional arrangements
- Over 50 new criminal offences
- Two chances to comment
- Process not an event

CYBERCRIMES & CYBERSECURITY BILL

Unlawful interception of data	Unlawful access	Personal information and financial information related offences
Unlawful acts in respect of software or hardware tools	Unlawful interference with data	Unlawful interference with computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure
Unlawful acts in respect of malware	Computer related fraud	Unlawful acquisition, possession, provision, receipt or use of passwords, access codes or similar data or devices
Computer related appropriation	Computer related extortion	Computer related forgery and uttering
Computer related terrorist activity and related offences	Computer related espionage and unlawful access to restricted data	Prohibition on dissemination of data message which advocates, promotes or incites hate, discrimination or violence
Prohibition on incitement of violence and damage to property	Prohibited financial transactions	Attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding, or procuring to commit offence
Harbouring or concealing person who commits offence	Infringement of copyright	

- **Procedural law mechanisms**
  - Search and seizure
  - Expedited data preservation direction
  - Data disclosure direction
  - Data preservation direction
  - Obligation to assist LEAs
  - Offence to release without a data disclosure direction

CYBERCRIME & CYBERSECURITY BILL

- **24 / 7 contact point**
  - Cybercrime Convention Art 35
  - Countries should designate a contact point for mutual assistance requests available 24/7 in order to ensure assistance in cyber related matters – aimed at international information exchange + providing technical assistance and advice, assisting with the preservation of data and collection of evidence, the provision of legal information and the location of suspects
  - Clause 49 of the Bill provides for the establishment of a 24/7 Point of Contact for SA.
- **National Cybercrime Centre**
  - dedicated structure to focus on cybercrime

- **SA Courts to have jurisdiction where**
  - the offence was committed in the SA
  - preparation for the offence or any part of the offence was committed in SA or where any result of the offence has had an effect in SA
  - the offence was committed in or outside SA by an SA citizen or a person with permanent residence in SA or by a person carrying on business in SA
  - the offence was committed on board any ship or aircraft registered in SA or on a voyage or flight to or from the SA when the offence was committed
  - the offence was committed outside SA and person charged is a citizen / resident / body of persons or arrested in SA
  - the offence was committed outside SA – irrespective of whether constitutes an offence where committed – then deemed to have been committed in SA if affects / intended to affect an SA public body + the offender is in SA + no extradition or application to extradite

- **Definition of "electronic communications service provider"**

"electronic communications service provider" means any—

(a) person who provides an electronic communications service under and in accordance with an electronic communications service licence issued to such person under Chapter 3 of the Electronic Communications Act, 2005 (Act No. 36 of 2005), or who is deemed to be licensed or exempted from being licensed as such in terms of the Electronic Communications Act, 2005;

(b) 'financial institution' as defined in section 1 of the Financial Services Board Act, 1990 (Act No. 97 of 1990); or

(c) person or entity who or which transmits, receives, processes or stores data—

(i) on behalf of the person contemplated in paragraph (a) or (b) or the clients of such a person; or

(ii) of any other person;

- **Section 64: proposed position with regard to ISPs**
- **64(1) Obligation to provide information & establish reporting mechanism**

64. (1) An electronic communications service provider must—

(*a*) take reasonable steps to inform its clients of cybercrime trends which affect or may affect the clients of such an electronic communications service provider;

(*b*) establish procedures for its clients to report cybercrimes with the electronic communications service provider; and

(*c*) inform its clients of measures which a client may take in order to safeguard himself or herself against cybercrime.

- **64(2) Obligation to report and preserve evidence**

(2) An electronic communications service provider that is aware or becomes aware that its computer network or electronic communications network is being used to commit an offence provided for in this Act must—

(a) immediately report the matter to the National Cybercrime Centre; and

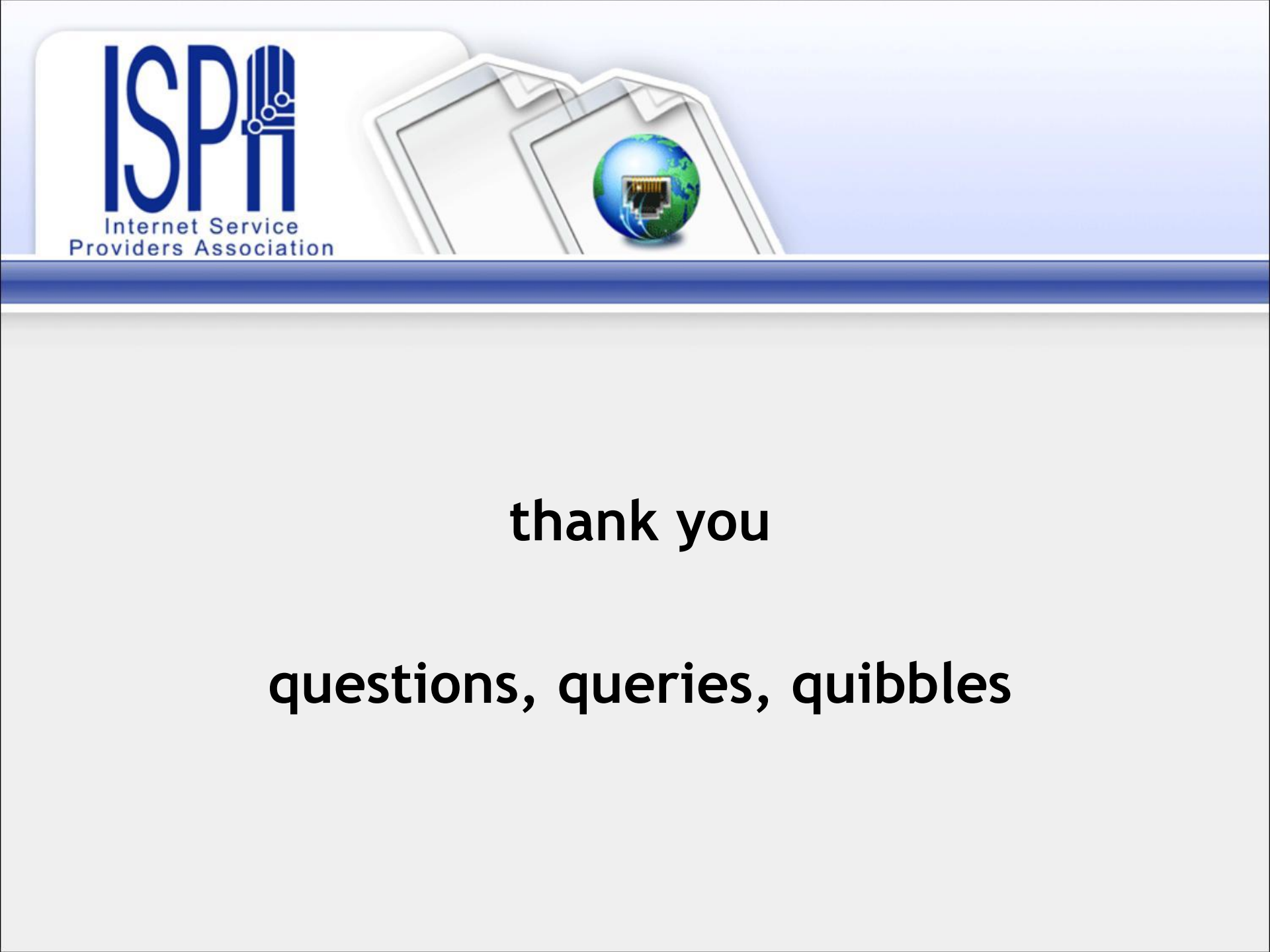
(b) preserve any information which may be of assistance to the law enforcement agencies in investigating the offence, including information which shows the communication's origin, destination, route, time date, size, duration and the type of the underlying services.

- **64(2) Sanctions and interface with National Cybercrime Centre**

(3) An electronic communications service provider which fails to comply with subsection (1) or (2), is guilty of an offence and is liable on conviction to a fine of R10 000, for each day on which such failure to comply, continues.

(4) The Cabinet member responsible for policing, in consultation with the Cabinet member responsible for the administration of justice, must make regulations regulating the manner in which an electronic communications service provider must report the use of its computer network or electronic communications network to commit an offence, to the National Cybercrime Centre.

- industry-driven initiative to identify infected machines, inform affected consumers that they may be at risk, provide support to enable those consumers to disinfect their machines + reduce their risk of re-infection.
- Objectives
  - instil a culture of cyber security within SA ISPs and their customers;
  - provide a consistent message in plain language in order to raise awareness of cyber security risks, educate users on steps that they can take to better protect themselves online, and to assist customers who may have infected machines;
  - encourage ISPs to identify compromised computers on their networks;
  - develop mechanisms for ISPs to share information and collaborate on cyber security concerns affecting SA ISPs; and
  - encourage ISPs to identify and report any cyber security issues that may affect SA's critical infrastructure or that may have a national security dimension
- Voluntary for all SA ISPs



thank you

questions, queries, quibbles