GLACY: LAUNCHING CONFERENCE
24-27 March 2014, Dakar, Senegal

Kingdom of Tonga

March 2014

OUTLINE

1. Milestones
    i. Cybercrime Workshop 2011
    ii. Submarine Fibre Optic Cable Project
    iii. Task Force
2. Content Regulation
3. Cybercrime
4. Future Considerations

1. Milestones

i. Cybercrime Workshop 2011

a. Regional Workshop for Pacific Island Countries – organized by the Secretariat of the Pacific Community (SPC) with the assistance of the Council of Europe (COE)

b. Established Working Group on Cybercrime – Ministry of Information and Communications (MIC), Ministry of Police, and Crown Law (now Attorney General's Office)

c. Negotiations on submarine fibre optic cable project between Government, the World Bank (WB), and the Asian Development Bank (ADB) – ICT regulatory reform, including cybercrime

1. Milestones

ii. Submarine Fibre Optic Cable Project

Implementing a project to improve regulatory environment for telecommunications following the launch of Tonga's first fibre optic cable in August 2013:

a. improve access to communications services
b. reflects Tonga's international commitments (e.g. WTO)
c. ensures it maximises confidence in the regulatory environment

1. Milestones

The regulatory environment include:

a. Institutional Structure to increase:
   i. Transparency
   ii. Information gathering
   iii. Enforcement Powers
b. Licensing – simplification and standardizing procedures and conditions
c. Interconnection and Access requirements
d. Competition Law – comprehensive competitive regimes
e. Consumer Protection - enhancing

1. Milestones

f. Content regulations – introducing a number of measures to provide greater public confidence and addressing potential negative impacts of faster broadband speed

g. Cybercrime – adjustments to existing legislations to reflect international and regional best practice

h. Technical Issues – radio spectrum, standards, etc

i. Universal access system

1. Milestones

iii. Task Force

Government recently established a Cyber Challenges Task Force to address the threats of cyberspace, comprising three main working groups:

a. Cyber-safety

b. Cyber-security

c. Cyber-crime

2. Content Regulations

Often considered to overlap with cybercrime

a. Social Regulations – Limit provisions in the Communications Act to apply only to content services (i.e. broadcasting, on-line services, etc.). Minister have ability to determine content standards
b. Take-down regime – of inappropriate content hosted in Tonga (on notice) – minimize risk of becoming a haven for hosting inappropriate content. Apply to contravening content standards, to defamatory material, and material forming the basis of an action of cyber-bullying/cyber-stalking

2. Content Regulations

c. Opt-out family friendly filtering – Internet Service Providers (ISPs) to apply content unlawful to possess, access, distribute or publish under the laws of Tonga. End users at least 18 years of age can opt-out

d. Mandatory filter – to block access to webpages and domains containing child pornography based on INTERPOL 'worst-off' list

e. Reporting Obligation – on ISPs to report pornography to Police.

3. Cybercrime

Extending the existing Tongan laws on cybercrime to reflect international and regional best practice

a. Existing regime comprises of :
   i. Computer Crime Act 2003
   ii. Criminal Offences Act
   iii. Pornography Control Act 2002

- Largely compliant with the Budapest Convention and best practice, with only a few areas need to be improved.
- Under pornography - amend to lift the age for defining a “child” to a person less than 18 years of age. Expressly criminalising accessing, obtaining or procuring child pornography

3. Cybercrime

- New offences criminalising:
  - procuring, grooming or engaging in sexual activity with a child by means of a communication service
  - computer-related forgeries, fraud (and theft), illegal remaining and data espionage, “spam”
  - obtaining, accessing or possessing pornographic material
  - unauthorised online gambling
- Introducing ‘safe harbours’ for certain service providers so they are not unintentionally caught by criminal conduct merely from transmitting data

3. Cybercrime

b. Law Enforcement Capabilities

- Existing law enforcement powers in the Computer Crimes Act 2003 and Mutual Assistance in Criminal Matters Act
- Largely compliant with the Budapest Convention and best practice. Only a few areas need to be improved
  - i. Enhancing law enforcement capabilities around:
    - preservation of data
    - production of information
    - use of remote forensic tools
    - interception warrants and orders in respect to assistance from foreign law enforcement officials
    - disclosure of information to foreign law enforcement agencies

3. Cybercrime

c. Interception Capabilities

- No requirement for interception capability
  - i. Requiring licensees to provide interception capability on particular kinds of communication services – but only once law enforcement agencies themselves have the capability necessary for receiving the intercepted data. Operators and law enforcement agencies would have to bear their own costs.
  - ii. Licensees will be able to impose cost-based fees for providing assistance to law enforcement

3. Cybercrime

d. Electronic Transactions (E-commerce)

i. Validity of electronic transaction

- Confirm that transactions in electronic form are valid.

ii. Recognition of electronic form

Allow electronic method to satisfy legal requirements for:

- a document be in writing;
- information to be recorded in writing;
- information to be given information in writing;
- for original documents;
- for a signature;
- for information to be retained (whether in electronic or non-electronic form);
- for information to be produced / or access to that information granted (whether in electronic or non-electronic form);

3. Cybercrime

iii. Time and place of an electronic communications

Set default rules about:

- time of dispatch and receipt of an electronic communication; and
- place of dispatch and receipt of an electronic communication.

3. Cybercrime

e. Intellectual Property Protection
   - Largely sufficient for protection in an online environment, with few enhancements:
     - Fair Use - Introducing a broad/flexible “fair use” style exception to copyright, to permit the use of copyright material for research, education and for other important online uses.
     - Safe Harbours - Ensuring that there are appropriate “safe harbour” provisions for protection and encourage investment in the telecommunications industry and online.
     - Enforcement Mechanisms - Clarifying the mechanisms by which owners of intellectual property can obtain a remedy that requires persons responsible for hosting infringing material to take it off the internet.

3. Cybercrime

f. Privacy and Data Protection

- Still to work out whether - ‘general privacy laws’ or ‘industry specific privacy laws’
- May incline to establish a policy which will:
  - help transition the government into adopting best practice in dealing with personal information (in anticipation of the eventual enactment of a general privacy law);
  - develop awareness of privacy issues in Tonga;
  - develop local experience and skills in complying with privacy laws; and
  - (at least for now), avoid the difficulties of implementing a full-fledged general privacy law (eg establishing an independent Privacy Commission and enforcement mechanisms).

4. Future Considerations

I. Resources
II. Trainings
III. International Cooperation
IV. ccTLD
V. Privacy and Data Protection
VI. Task Force – Working Group Activities