



TONGA'S CYBERCRIME LEGISLATION

Octopus Conference & Budapest Convention 10th
Anniversary Meeting: Cooperation against Cybercrime,
Council of Europe
Strasbourg, 21 - 23 November 2011

‘Aminiasi Kefu, Solicitor General



LEGISLATIVE FRAMEWORK

- Main legislation:
 - Computer Crimes Act 2003;
 - Based on Commonwealth Secretariat model legislation;
 - 2 main objectives:
 - Combat computer crime; and
 - Provide for collection and use of electronic evidence.
 - Evidence Act (some evidential provisions)



LEGISLATIVE FRAMEWORK

- **COMPUTER CRIMES ACT:**
 - Preliminary:
 - sets out 'Definitions'; and
 - the jurisdiction of the Act;
 - Offences:
 - illegal access of a computer system or protected computer;
 - Interference with data or a computer system;
 - Illegal interception of data;
 - Dealing in illegal devices
 - Procedural powers:
 - Search warrants;
 - Assistance to Tonga Police
 - Order production of data, disclosure of traffic data, preservation of data, interception of electronic communications and interception of traffic data.



LEGISLATIVE FRAMEWORK

- **Other general matters:**
 - Evidence of interference with a computer system or evidence generated from a computer system, is admissible in Court (section 16);
 - An Internet service provider is prohibited from disclosing it has received procedural orders under sections 11, 12, 13, 14 and 15 (section 17(1));
 - Protection of Internet service providers from legal action for disclosing data or information (section 17(2));
 - The power of the Minister for Communications to make regulations with the consent of Cabinet.



LEGISLATIVE FRAMEWORK

- **EVIDENCE ACT**

- Amended in 2003 to allow the admissibility of electronic evidence in legal proceedings;
- Amendments provide for the following:
 - Definitions of ‘electronic record’ and ‘electronic record system’ (section 2);
 - General admissibility of electronic records in evidence (section 54A);
 - Establishing the general scope of electronic records (section 54B);
 - The burden of proof on authentication of electronic records (section 54C);



LEGISLATIVE FRAMEWORK

- Proof of integrity of the electronic records to qualify as best evidence (section 54D);
- Allowance of presumption of integrity in certain circumstances (section 54E);
- Evidence of standards, usage or practice of how electronic records are recorded or preserved to determine admissibility (section 54F);
- Evidence relating to integrity, presumption of integrity or standards for electronic records can be provided by affidavit (section 54G);
- Agreement on admissibility of electronic record may be made (section 54H); and
- Admissibility of electronic signatures (section 54I).



LEGISLATIVE FRAMEWORK

- Other relevant laws: Criminal Offences Act
Pornography Control Act; Communications
Act 2000; Mutual Assistance in Criminal
Matters Act; and Extradition Act.



CYBERCRIME PROSECUTION

- Two cases since Computer Crimes Act 2003 was enacted:
 - Interference with data in a telecommunications company (adding phone credit to friends and family);
 - Illegal access of a protected computer of a electricity company (entering main server after termination of employment).
- ‘Data prosecution’ case was successful before a jury – received monetary fine and suspended imprisonment sentence;
- ‘Illegal access’ case withdrawn due to evidential problems



CYBERCRIME PROSECUTION

- Other cybercrime related cases :
 - Bank fraud (interference with data);
 - Forgery (use of computers to produce forged documents);
 - Counterfeit currency;
 - Credit card fraud (use of card without authorisation).
- Currently have mutual assistance requests involving requests for electronic data (Australia)



ISSUES

- Revision and updating of Tonga's legislative framework (e.g. SPAM);
- Limited forensic investigators;
- Training of investigators, prosecutors, practitioners and judges;
- Application of Computer Crimes Act to related offences such as bank fraud;
- Presentation of evidence before a lay jury.



WAY FORWARD

- **REVIEW AND UPDATE LEGISLATION:** Officials post-Workshop will review legislation, If required, seek policy direction on any amendments required, and enact amendments;
- **TRAINING:** Increase training of law enforcement officers (computer literacy)
- **ENFORCEMENT:** Encourage enforcement of cybercrime;
- **PUBLIC AWARENESS:** Increase public awareness.



RECENT DEVELOPMENTS

- Regional Workshop on Cybercrime in April 2011;
- Cabinet policy decision to review Computer Crimes Act – bring it up to date; and
- Policy paper being formulated for Cabinet policy decision to consider requesting accession to the Budapest Convention.



MALO 'AUPITO
THANK YOU