Establishment of Harmonized Policies for the ICT Market in the ACP Countries

Computer Crime and Cybercrime:

Southern African Development Community (SADC) Model Law

HIPSSA

Harmonization of ICT Policies in Sub-Saharan Africa

Disclaimer

This document has been produced with the financial assistance of the European Union. The views expressed may not necessarily reflect the official opinion of the European Union.

The designations employed and the presentation of material, including maps, do not imply the expression of any opinion whatsoever on the part of ITU concerning the legal status of any country, territory, city or area, or concerning the delimitations of its frontiers or boundaries. The mention of specific companies or of certain products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned.

Please consider the environment before printing this report.

Foreword

Information and communication technologies (ICTs) are shaping the process of globalisation. Recognising their potential to accelerate Africa's economic integration and thereby its greater prosperity and social transformation, Ministers responsible for Communication and Information Technologies meeting under the auspices of the African Union (AU) adopted in May 2008 a reference framework for the harmonization of telecommunications/ICT policies and regulations, an initiative that had become especially necessary with the increasingly widespread adoption of policies to liberalise this sector.

Coordination across the region is essential if the policies, legislation, and practices resulting from each country's liberalization are not to be so various as to constitute an impediment to the development of competitive regional markets.

Our project to 'Support for Harmonization of the ICT Policies in Sub-Sahara Africa' (HIPSSA) has sought to address this potential impediment by bringing together and accompanying all Sub-Saharan countries in the Group of African, Caribbean and Pacific States (ACP) as they formulate and adopt harmonized ICT policies, legislation, and regulatory frameworks. Executed by the International Telecommunication Union (ITU), co-chaired by the AU, the project has been undertaken in close cooperation with the Regional Economic Communities (RECs) and regional associations of regulators which are members of the HIPSSA Steering Committee. A global steering committee composed of the representatives of the ACP Secretariat and the Development and Cooperation – EurepeAid (DEVCO, European Commission) oversees the overall implementation of the project.

This project is taking place within the framework of the ACP Information and Telecommunication Technologies (@CP-ICT) programme and is funded under the 9th European Development Fund (EDF), which is the main instrument for providing European aid for development cooperation in the ACP States, and co-financed by the ITU. The @CP-ICT aims to support ACP governments and institutions in the harmonization of their ICT policies in the sector by providing high-quality, globally-benchmarked but locally-relevant policy advice, training and related capacity building.

All projects that bring together multiple stakeholders face the dual challenge of creating a sense of shared ownership and ensuring optimum outcomes for all parties. HIPSSA has given special consideration to this issue from the very beginning of the project in December 2008. Having agreed upon shared priorities, stakeholder working groups were set up to address them. The specific needs of the regions were then identified and likewise potentially successful regional practices, which were then benchmarked against practices and standards established elsewhere.

These detailed assessments, which reflect sub-regional and country-specific particularities, served as the basis for the model policies and legislative texts that offer the prospect of a legislative landscape for which the whole region can be proud. The project is certain to become an example to follow for the stakeholders who seek to harness the catalytic force of ICTs to accelerate economic integration and social and economic development.

I take this opportunity to thank the European Commission and ACP Secretariat for their financial contribution. I also thank the Economic Community of West African States (ECOWAS), West African Economic and Monetary Union (UEMOA), Economic Community of Central African States (ECCAS), Economic and Monetary Community of Central Africa (CEMAC), East African Community (EAC), Common Market for Eastern and Southern Africa (COMESA), Common Market for Eastern and Southern Africa (COMESA), Southern African Development Community (SADC), Intergovernmental Authority on Development (IGAD), Communication Regulators' Association of Southern Africa (CRASA), Telecommunication Regulators' Association of Central Africa (ARTAC), United Nations Economic Commission for Africa (UNECA), and West Africa Telecommunications Regulators' Association (WATRA), for their contribution to this work. Without political will on the part of beneficiary countries, not much would have been achieved. For that, I express my profound thanks to all the ACP governments for their political will which has made this project a resounding success.

Brahima Sanou
BDT, Director

Acknowledgements– Cybercrime

The present document represents an achievement of a regional activity carried out under the HIPSSA project ("Support to the Harmonization of ICT Policies in Sub-Sahara Africa") officially launched in Addis Ababa in December 2008.

In response to both the challenges and the opportunities of information and communication technologies' (ICTs) contribution to political, social, economic and environmental development, the International Telecommunication Union (ITU) and the European Commission (EC) joined forces and signed an agreement (ITU-EC Project) aimed at providing "Support for the Establishment of Harmonized Policies for the ICT market in the ACP", as a component of the Programme "ACP-Information and Communication Technologies (@CP-ICT)" within the framework of the 9th European Development Fund (EDF), i.e., ITU-EC-ACP project.

This global ITU-EC-ACP project is being implemented through three separate sub-projects customized to the specific needs of each region: Sub-Saharan Africa (HIPSSA), the Caribbean (HIPCAR), and the Pacific Island Countries (ICB4PAC).

As members of the HIPSSA Steering Committee co-chaired by the African Union's Commission (AUC) and the ITU, the Southern African Development Community (SADC) Secretariat and Communication Regulators' Association of Southern Africa (CRASA) Secretariat provided guidance and support to the consultants, Prof. Marco Gercke and Ms. Judith Tembo who prepared the draft document. This draft document was reviewed, discussed and validated by broad consensus by participants of the workshop organized in collaboration with CRASA and SADC Secretariats held in Gaborone, Botswana from 27 February to 3 March 2012. It was further adopted by the SADC Ministers responsible for Telecommunications, Postal and ICT at their meeting in Mauritius in November 2012.

ITU would like to thank the workshop delegates from the SADC ICT and telecommunications ministries, CRASA regulators, academia, civil society, operators and regional organizations for their hard work and commitment in producing the contents of the final report. The contributions from the SADC and CRASA Secretariats are gratefully acknowledged.

Without the active involvement of all of these stakeholders, it would have been impossible to produce a document such as this, reflecting the overall requirements and conditions of the SADC region while also representing international best practice.

The activities have been implemented by Ms. Ida Jallow, responsible for the coordination of the activities in Sub-Saharan Africa (HIPSSA Senior Project Coordinator), and Mr. Sandro Bazzanella, responsible for the management of the whole project covering Sub-Saharan Africa, Caribbean and the Pacific (ITU-EC-ACP Project Manager) with the overall support of Ms. Hiwot Mulugeta, HIPSSA Project Assistant, and of Ms. Silvia Villar, ITU-EC-ACP Project Assistant. The work was carried out under the overall direction of Mr. Cosmas Zavazava, Chief, Project Support and Knowledge Management Department. The document was developed under the direct supervision of the then HIPSSA Senior Project Coordinator, Mr. Jean-François Le Bihan, and has further benefited from the comments of the ITU Telecommunication Development Bureau's (BDT) Regulatory and Market Environment (RME), Special Initiatives and Strategies (SIS), and from ICT Applications and Cyber security (CYB) Divisions at the ITU. The team at ITU's Publication Composition Service was responsible for its publication.

Table of contents

Table of contents

Part I

PART I: Preliminary

Short Title

1. This legislation may be cited as the Computer Crime and Cybercrime Act, and shall come into force and effect [on xxx/ following publication in the *Gazette*].

Objective

2. The objective of a computer crime and Cybercrime legislation in [insert name of country] shall be the criminalization and investigation of computer and network related crime.

Definitions

3. (1) Access in relation to Sec. 4 means entering a computer system.

(2) Access provider means any natural or legal person providing an electronic data transmission service by transmitting information provided by or to a user of the service in a communication network or providing access to a communication network;

(3) Caching provider means any natural or legal person providing an electronic data transmission service by automatic, intermediate and temporary storing information, performed for the sole purpose of making more efficient the information's onward transmission to other users of the service upon their request;

(4) Child shall mean any person under the age of eighteen (18) years;

(5) Computer system (or information system) means a device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data or any other function;

(6) Computer data means any representation of facts, concepts, information (being either texts, audio, video or images) machine-readable code or instructions, in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

(7) Computer data storage medium means any article or material (for example, a disk) from which information is capable of being reproduced, with or without the aid of any other article or device;

(8) Child pornography means pornographic material that depicts presents or represents:

(a) a child engaged in sexually explicit conduct;

(b) a person appearing to be a child engaged in sexually explicit conduct; or

(c) images representing a child engaged in sexually explicit conduct;

this includes, but is not limited to, any audio, visual or text pornographic material.

A country may restrict the criminalisation by not implementing (b) and (c).

(9) Critical infrastructure means computer systems, devices, networks, computer programs, computer data, so vital to the country that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters.

(10) Device includes but is not limited to

(a) components of computer systems such as graphic cards, memory, chips and processors;
(b) storage components such as hard drives, memory cards, compact discs, tapes;
(c) input devices such as keyboards, mouse, track pad, scanner, digital cameras;
(d) output devices such as printer, screens.

(11) Electronic Communication means any transfer of signs, signals or computer data of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system.

(12) Hinder in relation to a computer system includes but is not limited to:
(a) cutting the electricity supply to a computer system; and
(b) causing electromagnetic interference to a computer system; and
(c) corrupting a computer system by any means; and
(d) inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data;

(13) Hosting provider means any natural or legal person providing an electronic data transmission service by storing of information provided by a user of the service;

(14) Hyperlink means characteristic or property of an element such as symbol, word, phrase, sentence, or image that contains information about another source and points to and causes to display another document when executed.

(15) Hyperlink provider means any natural or legal person providing one or more hyperlinks.

(16) Interception includes but is not limited to the acquiring, viewing and capturing of any computer data communication whether by wire, wireless, electronic, optical, magnetic, oral, or other means, during transmission through the use of any technical device.

(17) Multiple electronic mail messages mean a mail message including E-Mail and instant messaging sent to more than [thousand] recipients;

(18) Racist and xenophobic material means any material, including but not limited to any image, video audio recording or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

(19) Remote forensic tool means an investigative tool (including software or hardware) installed on or in relation to a computer system or part of a computer system and used to perform tasks that include but are not limited to keystroke logging or transmission of an IP-address;

(20) Seize includes:
(a) activating any onsite computer system and computer data storage media;
(b) making and retaining a copy of computer data, including by using onsite equipment;
(c) maintaining the integrity of the relevant stored computer data;

(d) rendering inaccessible, or removing, computer data in the accessed computer system;

(e) taking a printout of output of computer data; or

(f) seize or similarly secure a computer system or part of it or a computer-data storage medium.

(21) Internet service provider means a natural or legal person that provides to users services mentioned in sections 28 – 32 hereof;

(22) Traffic data means computer data that:

(a) relates to a communication by means of a computer system; and

(b) is generated by a computer system that is part of the chain of communication ; and

(c) shows the communication's origin, destination, route, time date, size, duration or the type of underlying services.

(23) Thing includes but not limited to:

(a) a computer system or part of a computer system;

(b) another computer system, if:

  (i) computer data from that computer system is available to the first computer system being searched; and

  (ii) there are reasonable grounds for believing that the computer data sought is stored in the other computer system;

(c) a computer data storage medium.

(24) Utilise shall include

(a) developing of a remote forensic tool; and

(b) adopting of a remote forensic tool; and

(c) purchasing of a remote forensic tool.

Part II

PART II: Offences

Illegal Access

4. A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, accesses the whole or any part of a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

Illegal Remaining

5. (1) A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, remains logged in a computer system or part of a computer system or continues to use a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

(2) A country may decide not to criminalize the mere unauthorized remaining provided that other effective remedies are available. Alternatively a country may require that the offence be committed by infringing security measures or with the intent of obtaining computer data or other dishonest intent.

Illegal Interception

6. (1) A person who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification, intercepts by technical means:

(a) any non-public transmission to, from or within a computer system; or

(b) electromagnetic emissions from a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

(2) A country may require that the offence be committed with a dishonest intent, or in relation to a computer system that is connected to another computer system, or by circumventing protection measures implemented to prevent access to the content of non-public transmission.

Illegal Data Interference

7. A person who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification, does any of the following acts:

(a) damages or deteriorates computer data; or

(b) deletes computer data ; or

(c) alters computer data; or

(d) renders computer data meaningless, useless or ineffective; or

(e) obstructs, interrupts or interferes with the lawful use of computer data; or

(f) obstructs, interrupts or interferes with any person in the lawful use of computer data; or

(g) denies access to computer data to any person authorized to access it; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

Data Espionage

8. (1) A person who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification obtains, for himself or for another, computer data which are not meant for him and which are specially protected against unauthorized access, commits an offence punishable, on

conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

(2) A country may limit the criminalisation to certain categories of computer data.

Illegal System Interference

9. (1) A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification:

(a) hinders or interferes with the functioning of a computer system; or

(b) hinders or interferes with a person who is lawfully using or operating a computer system;

commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

(2) A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justificationhinders or interferes with a computer system that is exclusively for the use of critical infrastructure operations, or in the case in which such is not exclusively for the use of critical infrastructure operations, but it is used in critical infrastructure operations and such conduct affects that use or impacts the operations of critical infrastructure the punishment shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

Illegal Devices

10 (1) A person commits an offence if the person:

(a) intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, produces, sells, procures for use, imports, exports, distributes or otherwise makes available:

(i) a device, including a computer program, that is designed or adapted for the purpose of committing an offence defined by other provisions of Part II of this law; or

(ii) a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed;

with the intent that it be used by any person for the purpose of committing an offence defined by other provisions of Part II of this law; or

(b) has an item mentioned in subparagraph (i) or (ii) in his or her possession with the intent that it be used by any person for the purpose of committing an offence defined by other provisions of part II of this law commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

(2) This provision shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 is not for the purpose of committing an offence established in accordance with other provisions of Part II of this law, such as for the authorized testing or protection of a computer system.

(3) A country may decide not to criminalize illegal devices or limit the criminalization to devices listed in a Schedule.

Part II

Computer-related Forgery

11. (1) A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification inputs, alters, deletes, or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

(2) If the abovementioned offence is committed by sending out multiple electronic mail messages from or through computer systems, the penalty shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

Computer-related Fraud

12. A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification causes a loss of property to another person by:

(a) any input, alteration, deletion or suppression of computer data;

(b) any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person the penalty shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

Child Pornography

13. (1) A person who intentionally, without lawful excuse or justification:

(a) produces child pornography for the purpose of its distribution through a computer system;

(b) offers or makes available child pornography through a computer system;

(c) distributes or transmits child pornography through a computer system;

(d) procures and/or obtain child pornography through a computer system for oneself or for another person;

(e) Possesses child pornography in a computer system or on a computer-data storage medium; and

(f) knowingly obtains access, through information and communication technologies, to child pornography,

commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

(2) It is a defence to a charge of an offence under paragraph (1) (b) to (1)(f) if the person establishes that the child pornography was for a bona fide law enforcement purpose.

Pornography

14. A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification makes pornography available to one or more children through a computer system or facilitates the access of children to pornography through a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

Identity-related crimes

15. A person who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification by using a computer system in any stage of the offence, intentionally transfers, possesses, or uses, without lawful excuse or justification, a means of identification of another person

with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a crime, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

Racist and Xenophobic Material

16. A person who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification

(a) produces racist and xenophobic material for the purpose of its distribution through a computer system;

(b) offers or makes available racist and xenophobic material through a computer system;

(c) distributes or transmits racist and xenophobic material through a computer system;

commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

Racist and Xenophobic Motivated Insult

17. A person who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification insults publicly, through a computer system,

(a) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or

(b) a group of persons which is distinguished by any of these characteristics commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

Denial of Genocide and Crimes Again Humanity

18. A person who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification distributes or otherwise makes available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

SPAM

19. (1) A person who, intentionally without lawful excuse or justification:

(a) intentionally initiates the transmission of multiple electronic mail messages from or through such computer system; or

(b) uses a protected computer system to relay or retransmit multiple electronic mail messages, with the intent to deceive or mislead users, or any electronic mail or Internet service provider, as to the origin of such messages, or

(c) materially falsifies header information in multiple electronic mail messages and intentionally initiates the transmission of such messages,

commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

(2) A country may restrict the criminalization with regard to the transmission of multiple electronic messages within customer or business relationships.

Disclosure of details of an investigation

20. An Internet service provider who receives an order related to a criminal investigation that explicitly stipulates that confidentiality is to be maintained or such obligation is stated by law and intentionally without lawful excuse or justification or in excess of a lawful excuse or justification discloses:

(a) the fact that an order has been made; or

(b) anything done under the order; or

(c) any data collected or recorded under the order;

commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

Failure to permit assistance

21. (1) A person other than the suspect who intentionally fails without lawful excuse or justification or in excess of a lawful excuse or justification to permit or assist a person based on an order as specified by sections 25 to 27 commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

(2) A country may decide not to criminalize the failure to permit assistance provided that other effective remedies are available.

Harassment utilizing means of electronic communication

22. A person, who initiates any electronic communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, using a computer system to support severe, repeated, and hostile behavior, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

Part III

PART III: Jurisdiction

Jurisdiction

23. This Act applies to an act done (offence committed) or an omission made:
   (a) in the territory of [enacting country]; or
   (b) on a ship or aircraft registered in [enacting country]; or
   (c) by a national of [enacting country] outside the jurisdiction ofany country; or
   (d) by a national of [enacting country] outside the territory of[enacting country], if the person's conduct would also constitute an offence under a law of the country where the offence was committed.

Part IV

PART IV: Electronic Evidence

Admissibility of Electronic Evidence

24. In proceedings for an offence against a law of [enacting country], the fact that evidence has been generated from a computer system does not by itself prevent that evidence from being admissible.

Part V

PART V: Procedural Law

Search and Seizure

25. (1) If a [judge] [magistrate] is satisfied on the basis of an application by a [law enforcement] [police] officer supported by [information on oath][affidavit] that there are reasonable grounds [to suspect] [to believe] that there may be in a place a thing or computer data:

(a) that may be material as evidence in proving an offence; or

(b) that has been acquired by a person as a result of an offence;

the [judge] [magistrate] [may] [shall] issue a warrant authorizing a [law enforcement] [police] officer, with such assistance as may be necessary, to enter the place to search and seize the thing or computer data including search or similarly access:

(i) a computer system or part of it and computer data stored therein; and

(ii) a computer-data storage medium in which computer data may be stored in the territory of the country.

(2) If a [law enforcement] [police] officer that is undertaking a search based on Sec. 25 (1) has grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, he shall be able to expeditiously extend the search or similar accessing to the other system.

(3) A [law enforcement] [police] officer that is undertaking a search is empowered to seize or similarly secure computer data accessed according to paragraphs 1 or 2.

Assistance

26. (1) Any person, who is not a suspect of a crime or otherwise excluded from an obligation to follow such order, but who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein that is the subject of a search under section 26 must permit, and assist if reasonably required and requested by the person authorized to make the search by:

(a) providing information that enables the undertaking of measures referred to in section 26;

(b) accessing and using a computer system or computer data storage medium to search any computer data available to or in the system;

(c) obtaining and copying such computer data;

(d) using equipment to make copies; and

(e) obtaining an intelligible output from a computer system in such a format that is admissible for the purpose of legal proceedings.

Production Order

27. If a [judge] [magistrate] is satisfied on the basis of an application by a [law enforcement officer] [police officer] that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the [judge] [magistrate] may order that:

(a) a person in the territory of [enacting country] in control of a computer system produce from the system specified computer data or a printout or other intelligible output of that data;or

Part V

(b) an Internet service provider in [enacting country] to produce information about persons who subscribe to or otherwise use the service.

Expedited preservation

28. If a [law enforcement] [police] officer is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, the [law enforcement] [police] officer may, by written notice given to a person in control of the computer data, require the person to ensure that the data specified in the notice be preserved for a period of up to seven (7) days as specified in the notice. The period may be extended beyond seven (7) days if, on an application a [judge] [magistrate]authorizes an extension for a further specified period of time.

Partial Disclosure of traffic data

29. If a [law enforcement] [police] officer is satisfied computer data is reasonably required for the purposes of a criminal investigation, the [law enforcement] [police] officer may, by written notice given to a person in control of the computer system, require the person to disclose [sufficient][relevant] traffic data about a specified communications to identify:

(a) the Internet service providers; and/or

(b) the path through which a communication was transmitted.

Collection of traffic data

30. (1) If a [judge] [magistrate]is satisfied on the basis of an application by a [law enforcement] [police] officer, supported by [information on oath] [affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] order a person in control of such data to:

(a) collect or record traffic data associated with a specified communication during a specified period; or

(b) permit and assist a specified [law enforcement] [police] officer to collect or record that data.

(2) If a [judge] [magistrate] is satisfied on the basis of an application by a [law enforcement] [police] officer, supported by [information on oath] [affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] authorize a [law enforcement] [police] officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means.

Interception of content data

31. (1) If a [judge] [magistrate] is satisfied on the basis of an application by a [law enforcement] [police] officer, supported by [information on oath] [affidavit] that there are reasonable grounds [to suspect][to believe] that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate][may] [shall]:

(b) order an Internet service provider whose service is available in [enacting country] through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or

Part V

Forensic Tool

32. (1) If a [judge] [magistrate] is satisfied on the basis of an application by a [law enforcement] [police] officer, supported by [information on oath] [affidavit] that in an investigation concerning an offence listed in paragraph 7 hereinbelow there are reasonable grounds to believe that essential evidence cannot be collected by applying other instruments listed in Part IV but is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate][may][shall] authorize a [law enforcement] [police] officer to utilize a remote forensic tool with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence. The application needs to contain the following information:

(a) suspect of the offence, if possible with name and address, and

(b) description of the targeted computer system, and

(c) description of the intended measure, extent and duration of the utilization, and

(d) reasons for the necessity of the utilization.

(2) Within such investigation it is necessary to ensure that modifications to the computer system of the suspect are limited to those essential for the investigation and that any changes if possible can be undone after the end of the investigation. During the investigation it is necessary to log

(a) the technical mean used and time and date of the application; and

(b) the identification of the computer system and details of the modifications undertaken within the investigation;.

(c) any information obtained.

Information obtained by the use of such tool need to be protected against any modification, unauthorized deletion and unauthorized access.

(3) The duration of authorization in section 32 (1) is limited to [3 months]. If the conditions of the authorization is no longer met, the action taken are to stop immediately.

(4) The authorization to install the tool includes remotely accessing the suspects computer system.

(5) If the installation process requires physical access to a place the requirements of section 25 need to be fulfilled.

(6) If necessary a police officer may pursuant to the order of court granted in (1) above request that the court order an internet service provider to support the installation process.

(7) [List of offences]

(8) A country may decide not to implement section 33.

Part VI

PART VI: Liability

No Monitoring Obligation

33. When providing the services contemplated in this Chapter there is no general obligation on an Internet service provider to monitor the data which it transmits or stores; or actively seek facts or circumstances indicating an unlawful activity.

The [Minister] may, subject to the provisions of any other law, prescribe procedures for service providers to

(a) inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service; and

(b) to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service.

Access Provider

34. (1) An access provider is not criminally liable for providing access and transmitting information on condition that the provider:

(a) does not initiate the transmission;

(b) does not select the receiver of the transmission; or

(c) does not select or modify the information contained in the transmission.

(2) The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

Hosting Provider

35. (1) A hosting provider is not criminally liable for the information stored at the request of a user of the service, on condition that:

(a) the hosting provider expeditiously removes or disables access to the information after receiving an order from any public authority or court of law to remove specific illegal information stored; or

(b) the hosting provider, upon obtaining knowledge or awareness about specific illegal information stored by other ways than an order from a public authority, expeditiously informs a public authority to enable them to evaluate the nature of the information and if necessary issue an order to remove the content.

(2) Paragraph 1 shall not apply when the user of the service is acting under the authority or the control of the hosting provider.

(3) If the hosting provider is removing the content after receiving an order pursuant to paragraph 1 he is exempted from contractual obligations with his customer to ensure the availability of the service.

Caching Provider

36. A caching provider is not criminally liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other users of the service upon their request, on condition that:

(a) the caching provider does not modify the information;

(b) the caching provider complies with conditions of access to the information;

(c) the caching provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;

(d) the caching provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and

(e) the caching provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

Hyperlinks Provider

37. An Internet service provider who enables the access to information provided by third person by providing an electronic hyperlink is not liable for the information if

(a) the internet service provider expeditiously removes or disables access to the information after receiving an order from any public authority or court to remove the link; and

(b) the internet service provider, upon obtaining knowledge or awareness about specific illegal information stored by other ways than an order from a public authority, expeditiously informs a public authority to enable them to evaluate the nature of the information and if necessary issue an order to remove the content.

Search Engine Provider

38. An Internet service provider who makes and/or operates a search engine that either automatically or based on entries by others creates and index of Internet-related content or makes available electronic tools to search for information provided by third party is not liable for search results on condition that the provider:

1. does not initiate the transmission; and
2. does not select the receiver of the transmission; and
3. does not select or modify the information contained in the transmission.