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

Electronic Crimes: Knowledge-Based Report

(Skeleton)

ICB4PAC

Capacity Building and ICT Policy, Regulatory and Legislative Frameworks for Pacific Island Countries

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

Electronic Crimes: Knowledge-based Report

(Skeleton)

ICB4PAC

Capacity Building and ICT Policy, Regulatory and Legislative Frameworks for Pacific Island Countries

Disclaimer

This document has been produced with the financial assistance of the European Union. The views expressed herein do not necessarily reflect the views 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. This Report has not been through editorial revision.

Please consider the environment before printing this report.

Foreword

Information and communication technologies (ICTs) are serving as the most important driving force behind the Pacific Islands' economic and social integration into the wider global community.

In light of the huge changes that are taking place and mindful of the need to shape them in ways that best reflect the aspirations of the individual islands societies -- each with their unique heritage -- 15 Pacific countries in the Group of African, Caribbean and Pacific States (ACP) have come together to develop and promote the use of harmonised ICT policies, legislation and regulatory frameworks.

This cooperation has taken the form of a project entitled "Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island countries" (ICB4PAC). Executed by the International Telecommunication Union (ITU), the project has been undertaken in close collaboration with the Pacific Islands Forum Secretariat (PIFS), Secretariat of the Pacific Community (SPC), Pacific Islands Telecommunication Authority (PITA), and the Pacific ICT Regional Regulatory Centre (PIRRC), with the support of the University of the South Pacific (USP). A global steering committee composed of the representatives of the ACP Secretariat and the Development and Cooperation - EuropeAid (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. ICB4PAC has given special consideration to this issue from the very beginning of this project in November 2009. Having agreed upon shared priorities, stakeholders reviewed the methodology and governance for implementing the project. The specific needs of the region were then identified and likewise potentially successful regional practices; these were then benchmarked against practices and standards established elsewhere.

These detailed assessments (knowledge-based reports), which reflect 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 for other regions to follow as they too 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 Pacific Islands Forum Secretariat (PIFS) and the Secretariat of the Pacific Community (SPC) 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

This report documents the achievements of the regional activities carried out under the ICB4PAC project, Capacity Building and ICT Policies, Regulations and Legislative Frameworks for Pacific Island countries, officially launched in Fiji in November 2009.

In response to both the challenges and the opportunities from 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 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: Pacific island countries (ICB4PAC), the Caribbean (HIPCAR) and sub-Saharan Africa (HIPSSA).

The ICB4PAC focal points and project coordinator provided guidance and support to a consultant, Professor Marco Gercke. He conducted an assessment of cybercrime legislation in the ACP member countries of the Pacific Island region. The resulting draft assessment report was reviewed, discussed and adopted by broad consensus by participants at the first workshop to discuss and agree its findings (Vanuatu, March 2011).

ITU would like to especially thank the workshop delegates from the Pacific Island ICT and telecommunication ministries, regulators, academia, civil society, operators and regional organizations for their hard work and commitment in producing the contents of this report. These include the Pacific Island Forum Secretariat (PIFS), University of the South Pacific (USP), Secretariat of the Pacific Communities (SPC), Pacific ICT regional regulatory center (PIRRC), and Pacific Island Telecommunications Association (PITA). This broad base of public sector participation representing different sectors allowed the project to benefit from a cross-section of views and interests.

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

The activities have been implemented by Ms Gisa Fuatai Purcell, responsible for the coordination of the activities in the Pacific (ICB4PAC 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 Reshmi Prasad, ICB4PAC 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 (PKM) Department.. The document has further benefited from comments of the ITU Telecommunication Development Bureau's (BDT) ICT Applications and Regulatory Monitoring and Evaluation (RME) Division. Support was provided by Mrs Eun-Ju Kim, Regional Director for Asia and the Pacific. The team at ITU's Publication Composition Service was responsible for its publication.

Table of Contents

Page

Table of contents

PART I. DEFINITIONS

Definitions **1.** **(1)** "*Access provider*" means any person providing any electronic communication 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;

(2) "*Caching provider*" means any 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;

(3) "*Child*" means any person under the age of [eighteen] years;

(4) "*Child pornography*" means material that:

(a) depicts or presents a child engaged in sexually explicit conduct; or

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

(c) realistically represents a person appearing to be child engaged in sexually explicit conduct;

this includes, but *is* not limited to, any visual (images, animations or videos), audio or text material.

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

(5) "*Critical infrastructure*" means electronic systems, devices, networks, computer programs, electronic data, vital for

(i) the security, defense or international relations of [enacting country]; or

(ii) the existence or identity of a confidential source of information relating to the enforcement of criminal law; or

(iii) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, courts, public transportation, public key infrastructure, payment systems infrastructure or e-commerce infrastructure; or

(iv) the protection of public safety including systems related to essential emergency services such as police, civil defense and medical services;

(v) the purpose declared as such by the [appropriate ministry or office of enacting country] in accordance with the prescribed procedure; or

(vi) containing any data or database protected as such, by any other law;

where the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on the country.

(6) *"Cyber stalking"* means repeated coercion, intimidation, harassment, insult or annoyance through electronic system or electronic devices;

(7) *"Electronic"* includes but not limited to electrical, digital, analogue, magnetic, optical, biochemical, electrochemical, electromechanical, electromagnetic, radio electric or wireless technology;

Part I.

(8) *"Electronic communication"* means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by electronic means;

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

(10) *"Electronic device"* means any hardware or equipment which performs one or more specific functions and operates on any form or combination of electrical energy and includes but is not limited to

(a) components of electronic systems such as computer, graphic cards, mobile phones, memory, chips;

(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 mail message" means any data generated by an electronic system for a unique electronic mail address;

(12) "*Electronic 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.

(13) *"Electronic system"* means any electronic device or a group of interconnected or related devices, one or more of which, pursuant to a program or manual or any external instruction, performs automatic processing of information or electronic data and may also include a permanent, removable or any other electronic storage medium;

(14) "*Hinder"* in relation to an electronic system includes but is not limited to:

(a) cutting the electricity supply to an electronic system; or

(b) causing electromagnetic interference to an electronic system; or

(c) corrupting an electronic system by any means; or

(d) damaging, deleting, deteriorating, altering or suppressing electronic data;

(15) "*Hosting provider"* means any person providing an electronic data transmission service by storing of information provided by a user of the service;

(16) "*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;

(17) "*Hyperlink provider*" means any person providing one or more hyperlinks.

(18) "*Information*" includes text, message, data, voice, sound, database, video, signals, software, computer programs, codes including object code and source code;

Part I.

(19) "*Interception"* means tapping into an electronic communication not directed to the one who is tapping in including but is not limited to the acquiring, viewing and capturing of any electronic communication whether by wire, wireless, electronic, optical, magnetic, or other means, during transmission through the use of any technical device;

(20) "*Internet Service Provider"* means a person that provides to users services mentioned in sections 34-38;

(21) "*Remote Forensic Tool"* means an investigative tool such as software or hardware installed on or applied with regard to an electronic system and used to perform tasks that include but are not limited to keystroke logging or transmission of an IP-address;

(22) "*Seize"* includes:

(a) activating any onsite electronic system and electronic storage media;

(b) making and retaining a copy of electronic data, including by using onsite equipment;

(c) maintaining the integrity of the relevant stored electronic data;

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

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

(f) secure an electronic system or part of it or an electronic storage medium;

(23) "*Spam"* means the unsolicited transmission of a harmful, fraudulent, misleading or illegal electronic mail message to any person or causing an electronic system to show such message for commercial or illegal purpose.

(24) "*Traffic data*" means electronic data that:

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

(b) is generated by an electronic 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;

(25) "*Thing"* includes but not limited to:

(a) an electronic system or part of an electronic system;

(b) another electronic system, if:

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

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

(c) an electronic data storage medium;

PART II. SUBSTANTIVE CRIMINAL LAW

Illegal Access

2. **(1)** 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 an electronic 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 access provided that other effective remedies are available. Furthermore a country may require that the offence be committed by infringing security measures or with the intent of obtaining electronic data or other dishonest intent.**)**

(3 If the act described in Sec. 2 (1) includes intentional access to critical infrastructure the person commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.**)**

Illegal Remaining

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

Illegal Interception

4. **(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 an electronic system; or

(b) electromagnetic emissions from an electronic 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 an electronic system that is connected to another electronic system, or by circumventing protection measures implemented to prevent access to the content of non-public transmission.

(3) A country may criminalize the unlawful use of information received during an interception.]

Illegal Data Interference

5. A person who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification, interferes with an electronic data owned or managed by someone else by doing any of the following acts:

(a) damages or deteriorates electronic data; or

(b) deletes electronic data; or

(c) alters electronic data; or

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

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

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

Part II.

(g) denies access to electronic 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 **6.** **(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, electronic data which are not meant for him, and which are not public or 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 electronic data or not require that data are specially protected against unauthorized access.]

Illegal System Interference **7.** **(1)** A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification:

(a) [Hinders/denies or interferes with the functioning of an electronic system; or

(b) Hinders/denies or interferes with a person who is lawfully using or operating an electronic 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 justification hinders or interferes with an electronic 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 **8.** **(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 software, electronic system or an electronic device, 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 password, access code or similar data by which the whole or any part of an electronic system or electronic data is capable of being accessed;

that is contained in a schedule published by the [ministry] 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.

Part II.

(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 an electronic system.

[**(3)** A country may decide not to criminalize acts related to illegal devices provided that other effective remedies are available.

(4) The [*relevant Government authority*] may, be authorized to edit the list and published it in the [*Gazette*].]

Computer-related Forgery

10. 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 electronic data;

(b) any interference with the functioning of an electronic 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

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

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

(b) offers or makes available child pornography through an electronic system;

(c) distributes or transmits child pornography through an electronic system;

(d) procures and or obtains child pornography through an electronic system for oneself or for another person;

(e) Possesses child pornography in an electronic system or on an electronic storage medium; and

(f) knowingly obtains access, through electronic system, 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 defense to a charge of an offence under paragraph (1) (b) to (1)(f) if the person establishes that the child pornography was offered, distributed, procured or kept for bona fide religious, research, law enforcement or medical purposes. If child pornography was stored for such purpose, the authorized persons need to ensure that it is deleted as soon as it is not legally required anymore.

Pornography

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

(a) produces pornography for the purpose of its distribution through an electronic system;

(b) offers or makes available pornography through an electronic system;

(c) distributes or transmits pornography through an electronic system;

(d) procures and or obtains pornography through an electronic system for oneself or for another person;

(e) Possesses pornography in an electronic system or on an electronic storage medium; and

(f) knowingly obtains access, through electronic system, to 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 defense to a charge of an offence under paragraph (1) if the person establishes that the pornography was produced, offered, distributed, procured or kept for bona fide religious, research, law enforcement or medical purposes.

Identity-related crimes

13. A person who, without lawful excuse or justification or in excess of a lawful excuse or justification by using an electronic 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.

SPAM

14. **(1)** A person who, without lawful excuse or justification:

(a) initiates the transmission of spam; or

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

(c) materially falsifies header information in spam 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 mail messages within customer or business relationships. A country may decide not to criminalize the conduct in section 14 (1) (a) provided that other effective remedies are available.]

Disclosure of details of an investigation

15. A service provider including its employees, 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 provide assistance

16. **(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 provide or assist a person presenting an order as specified by sections 24 to 28 commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

Part II.

[**(2)** A country may decide not to criminalize the failure to provide assistance subject to other remedies being available.]

Cyber Stalking **17.** A person, who initiates directly or indirectly any electronic communication, to do cyber stalking 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 harassment provided that other effective remedies are available.]

Illegal Gambling **18.** A country may criminalize illegal online gambling.

Solicitation of Children **19.** A person who intentionally, through electronic system proposes to a child, to meet him or her, with the intent of sexually exploiting the child, whether or not such proposal has been followed by material acts, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

Defamation **20.** A country may criminalize defamation committed by means of electronic system.

Racial and religious offences **21.** A country may criminalize racial and religious acts committed by using means of electronic systems.

Aiding, abetting, attempt and corporate liability **22.** A country may criminalize aiding and abetting as well the attempt to commit the crimes in Part II. Countries may further consider introducing corporate liability.

PART III. JURIDICTION

Jurisdiction **23.** This Act applies to an act done or an omission made:

(a) in the territory of [enacting country]; or

(b) 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; or

(c) by a national of [enacting country] outside the jurisdiction of any country.

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 an electronic system does not by itself prevent that evidence from being admissible.

PART V. PROCEDURAL LAW

Search and Seizure

25. **(1)** If a [judge][magistrate][registrar]on application by a [police officer][law enforcement officer][regulator] is satisfied on the basis of [sworn evidence] [affidavit][information] that there are reasonable grounds [to suspect] [to believe] that there may be in a place an electronic device or electronic 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][registrar] may issue a warrant authorizing a [police officer][law enforcement officer][regulator], with such assistance as may be necessary, to enter the place to search and seize the electronic device or electronic data including search or similar access:

(i) an electronic system or part of it and electronic data stored therein; and

(ii) an electronic storage medium in which electronic data may be stored in the territory of the country.

(2) Any person who makes a search or seizure under this section, shall at the time or as soon as practicable:

(a) make a list of what has been seized, with the date and time of seizure; and

(b) give a copy of that list to — [to be determined by enacting country]

(i) the occupier of the premises; or

(ii) the person in control of such electronic devices.

(3) Subject to subsection (4), on request, any [police officer][law enforcement officer][regulator] or another authorized person shall:

(a) permit a person who had the custody or control of the electronic devices, or someone acting on their behalf to access and copy electronic data on the system; or

(b) give the person a copy of the electronic data.

(4) The [police officer][law enforcement officer][regulator] or another authorized person may refuse to give access or provide copies if he or she has reasonable grounds for believing that giving the access, or providing the copies may —

(a) constitute a criminal offence; or

(b) prejudice:

(i) the investigation in connection with which the search was carried out;

(ii) another ongoing investigation; or

(iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations.

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

Part V.

(6) [Police officer][law enforcement officer][regulator] that is undertaking a search is empowered to seize or similarly secure electronic data accessed according to paragraphs 1 or 2.

Assistance

26. A person who is not a suspect of a crime but is in possession or control of an electronic device or electronic data that is the subject of a search under Sec. 25 (1) shall at his own cost permit, and assist if required, the [police officer][law enforcement officer][regulator] making the search to —

(a) access and use an electronic device or electronic data;

(b) obtain and copy that electronic data;

(c) use an electronic device to make copies; and

(d) obtain an intelligible output from an electronic device in a format that can be read.

Production Order

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

(a) a person in control of an electronic device or electronic system of electronic devices to produce specified electronic data or printout of such information; and

(b) a service provider to produce information about persons who subscribe to or use their services.

Expedited preservation

28. **(1)** Where a [police officer][law enforcement officer][regulator] is satisfied that:

(a) electronic data stored in an electronic device is reasonably required for the purpose of a criminal investigation; and

(b) there is a risk that the data may be destroyed or rendered inaccessible;

the [police officer][law enforcement officer][regulator] may, by written notice given to a person in control of the electronic device, require the person to ensure that the data specified in the notice be preserved for a period of up to 7 days as specified in the notice.

(2) A [judge][magistrate][registrar] may upon application authorize an extension not exceeding 14 days.

Partial Disclosure of traffic data

29. If a [judge][magistrate][registrar] is satisfied on the basis of an application by a [police officer][law enforcement officer][regulator] that specified data stored in an electronic device or system of electronic devices is required for the purpose of a criminal investigation or criminal proceedings, the [judge][magistrate][registrar] may order such person to disclose sufficient traffic data about a specified communication

to identify:

(a) the service providers; and

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

Part V.

Collection of traffic data

30. **(1)** If a [judge][magistrate][registrar] on application by a [police officer][law enforcement officer][regulator] is satisfied on the basis of [sworn evidence] [affidavit][information] that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the [judge][magistrate][registrar] may, by written notice given to a person in control of such data, request that person to:

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

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

(2) If a [judge][magistrate][registrar] on application by a [police officer][law enforcement officer][regulator] is satisfied on the basis of [sworn evidence] [affidavit][information] that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the [judge][magistrate] [registrar] may authorize any [police officer][law enforcement officer][regulator] to collect or record traffic data associated with a specified communication during a specified period through application of technical means.

[**(3)** A country may decide not to implement section 30.]

Lawful Interception

31. If a [judge][magistrate][registrar] on application by a [police officer][law enforcement officer][regulator] is satisfied on the basis of [sworn evidence] [affidavit][information] that content of electronic communications is reasonably required for the purposes of a criminal investigation, the [judge][magistrate][registrar] may:

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

(b) authorize a [police officer][law enforcement officer][regulator] to collect or record that data through application of technical means.

[**(2)** A country may decide not to implement section 31.]

Forensic Tool

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

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

(b) description of the targeted electronic 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 electronic system of the suspect or his service provider 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 electronic system and details of the modifications undertaken within the investigation; and

(c) any information obtained.

Any such information obtained by the use of such software 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 are no longer met, the action taken are to stop immediately.

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

(5) If necessary [police officer][law enforcement officer][regulator] may pursuant to the order granted in (1) above requests that the [judge][magistrate][registrar] order a service provider to support the installation process.

(6) [List of offences]

[**(7)** A country may decide not to implement section 32.]

PART VI. LIABILITY

No Monitoring Obligation

33. **(1)** Internet service providers do not have a general obligation to monitor the information which they transmit or store on behalf of another, nor do they have a general obligation to actively seek facts or circumstances indicating illegal activity to avoid criminal liability. This provision does not affect the possibility for a [court][other competent authority] to require an Internet service provider to terminate or prevent an infringement based on any law enacted by Parliament within [enacting country].

(2) A country may decide to enact specific monitoring obligations by law or regulations.

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 takes appropriate action to remedy and inform [the relevant 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 pursuant to paragraph 1 he is exempted from contractual obligations with his customer to ensure the availability of the service.

(4) A country may decide to specify which public authority shall be responsible for receiving information based on section 35 (1)(b) by law or regulations.

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. A Hyperlink 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 Hyperlink provider expeditiously removes or disables access to the information after receiving an order from a [court][other relevant authority]to remove the link; and

(b) the Hyperlink provider upon obtaining knowledge or awareness about specific illegal information stored by other ways than an order from a [court][other relevant authority], expeditiously informs any[court][other relevant 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. A provider who makes 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 conditions 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.

Registration of Users

39. A country may decide to enact obligations of a service provider to require a registration of users prior to the use of the service, either through this legislation or through other regulatory instruments under relevant telecommunications law.

International Telecommunication Union
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva 20

E-mail: bdtmail@itu.int
www.itu.int/ITU-D/projects/ITU_EC_ACP/

Geneva, 2013