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

Interception of Communications: Assessment Report

HIPCAR

Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean

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

Interception of Communications:

Assessment Report

HIPCAR

Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean

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 shaping the process of globalisation. Recognising their potential to accelerate the Caribbean region's economic integration and thereby its greater prosperity and social transformation, the Caribbean Community (CARICOM) Single Market and Economy has developed an ICT strategy focusing on strengthened connectivity and development.

Liberalisation of the telecommunication sector is one of the key elements of this strategy. Coordination across the region is essential if the policies, legislation, and practices resulting from each country's liberalisation are not to be so various as to constitute an impediment to the development of a regional market.

The project 'Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures' (HIPCAR) has sought to address this potential impediment by bringing together and accompanying all 15 Caribbean countries in the Group of African, Caribbean and Pacific States (ACP) as they formulate and adopt harmonised ICT policies, legislation, and regulatory frameworks. Executed by the International Telecommunication Union (ITU), the project has been undertaken in close cooperation with the Caribbean Telecommunications Union (CTU), which is the chair of the HIPCAR Steering Committee. 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. HIPCAR 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 region were then identified and likewise potentially successful regional practices, which were then benchmarked against practices and standards established elsewhere.

These detailed assessments, 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 Caribbean Community (CARICOM) Secretariat and the Caribbean Telecommunication Union (CTU) Secretariat 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

The present document represents an achievement of the regional activities carried out under the HIPCAR project "Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures", officially launched in Grenada in December 2008. It is a companion document to the Model Policy Guidelines and Legislative Texts on this HIPCAR area of work[1].

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: the Caribbean (HIPCAR), sub-Saharan Africa (HIPSSA) and the Pacific Island Countries (ICB4PAC).

The HIPCAR Steering Committee – chaired by the Caribbean Telecommunications Union (CTU) – provided guidance and support to a team of consultants including Ms. Karen Stephen-Dalton and Mr. Gilberto Martins de Almeida, who prepared the initial draft documents. The documents were then reviewed, finalized and adopted by broad consensus by the participants at the First Consultation Workshop for HIPCAR's Working Group 1 on ICT Policy and Legislative Framework on Information Society Issues, held in Saint Lucia on 8-12 March 2010. Based on the assessment report, Model Policy Guidelines and Legislative Texts were developed, reviewed and adopted by broad consensus by the participants at the Second Consultation Workshop held in Barbados on 23-26 August 2010.

ITU would like to especially thank the workshop delegates from the Caribbean ICT and telecommunications ministries and regulators as well as their counterparts in the ministries of justice and legal affairs, academia, civil society, operators, and regional organizations, for their hard work and commitment in producing the contents of the HIPCAR model texts. The contributions from the Caribbean Community Secretariat (CARICOM) and CTU are also gratefully acknowledged.

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

The activities have been implemented by Ms Kerstin Ludwig, responsible for the coordination of activities in the Caribbean (HIPCAR Project Coordinator), and Mr Sandro Bazzanella, responsible for the management of the whole project covering sub-Saharan Africa, the Caribbean and the Pacific (ITU-EC-ACP Project Manager) with the overall support of Ms Nicole Darmanie, HIPCAR Project Assistant, and of Ms Silvia Villar, ITU-EC-ACP Project Assistant. The work was carried 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 Cybersecurity Division (CYB) and Regulatory and Market Environment Division (RME). Support was provided by Mr. Philip Cross, ITU Area Representative for the Caribbean. The team at ITU's Publication Composition Service was responsible for its publication.

[1] HIPCAR Model Policy Guidelines and Legislative Texts, including implementation methodology, are available at www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html

Table of Contents

Page

Section I:
Introduction

Given the key role of communications[2] in an Information Society context, interception of communication has been an essential mechanism in the protection of States and individuals, under certain circumstances. In view of the fact that its exercise may collide with privacy and other important rights, definition on the criteria which shall determine or circumscribe its use requires proper policy-making and legislative drafting.

In accordance with ITU's Toolkit for Cybercrime Legislation[3], "interception" is defined as "the acquisition, viewing, capture, or copying of the contents or a portion thereof, of any communication, including content data, computer data, traffic data, and/or electronic emissions thereof, whether by wire, wireless, electronic, optical, magnetic, oral, or other means, *during transmission* through the use of any electronic, mechanical, optical, wave, electromechanical, or other device."[4]

Such definition explains the broad scope of "interception" as well of "communication" subject to it, which includes "content" (information communicated), and "traffic" (data relating to communication[5]). It also outlines different means of communication which may be intercepted. Naturally, Internet-based communication, and especially, cybercrime, constitute an important portion of interception activities, from quantitative and complexity standpoints.

European Directives 02/58/EC and 06/24/EC also provide relevant inputs for the understanding on how comprehensive an interception of communication may be. The concepts of "data"[6] and of "location data"[7] are of particular interest in such connection.

---

2 Such expression is defined by European Directive 02/58/EC, in its Article 2, "d", as "any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information."

3 Available at www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf, and developed in conjunction with the American Bar Association's Privacy & Computer Crime Committee, Section of Science & Technology Law.

4 Section 1 – Definitions, item "k".

5 The Budapest Convention, administered by the Council of Europe, has defined "traffic data", in Article 1, "d", as "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service"; on its turn, "computer data" is therein defined, in letter "b" of Article 1, as "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function". Traffic data is also defined in Article 2, "b", of the European Directive 02/58/EC as "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof."

6 Defined in Article 2, "a", of the European Directive 06/24/EC as "traffic data and location data and the related data necessary to identify the subscriber or user."

7 Defined in Article 2, "c", of the European Directive 06/24/EC as "any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service".

Section I

Interception of communication may be legally admissible and enforceable. Generally speaking, lawful interception comprises obtaining communication data upon lawful mandate, for purposes of analysis or of evidence. Lawful mandate in this area often relate to cyber-security and to protection of communications infrastructure. Lawful interception plays a crucial role in helping law enforcement agencies, regulatory or administrative agencies, and intelligence services, in combating crime and the increasing sophistication of today's criminals. Lawful interception represents an *indispensable means of gathering information against ruthless criminals*[8].

The changes in the telecommunications and postal markets, and the wide expansion in the nature and range of services available in most States are noteworthy. Mobile phones have developed to the mass ownership which is seen today, communications via the Internet have grown dramatically in the last few years and this continues to be the case, and the postal sector is developing rapidly with the growth in the number of companies offering parcel and document delivery services. Criminals (including terrorists) have been quick to exploit these extraordinary changes in the communications sector for their criminal activities while the legislation in many States have failed to keep up with these changes and risk the degrading of the capability of the law enforcement, security and intelligence agencies.

The serious criminal and security threats facing the worldwide community have caused many countries including Australia, the United States, the United Kingdom, Saint Lucia and Jamaica to enact legislation that requires electronic communications service providers to be capable of carrying out lawful interception and to regulate interception of communications activities.

For interception of communications to be lawful it must be conducted in accordance with national law, which may regulate either private or official interception of communication. Lawfulness of private interception of communication is restricted to a limited number of situations, which may include, for instance, electronic monitoring of employees in the workplace. National law may deal with private interception of communication in the context of labor relationship, privacy rights, or otherwise.

This report focuses primarily in official interception of communication. That means interception carried out by following due process of law, including the grant of proper authorization by competent authorities.

The provision of national law *"will ensure that criminals can no longer be able to take advantage of new technologies to hide their illegal activities from the law*[9]*"*.

---

[8] Notes on OECS Interception of Communications Bill, page 6 found at http://unpan1.un.org/intradoc/groups/public/documents/TASF/UNPAN024635.pdf www.itu.int/dms_pub/itu-t/oth/23/01/T23010000060002PDFE.pdf

[9] Honourable Anne McLellan, Deputy Prime Minister and Minister of Public Safety and Emergency Preparedness, introducing legislation lawful interception of communications in Canada.

Section II:
Executive Summary

This Assessment Report has been prepared in accordance with Phase 1 of Work Plan for the Working Group on ICT Legislative Framework – Information Society Issues under the HIPCAR[10] Project, which makes provision for a critical assessment report of Interception of Communications Acts existing in a number of States (the "Beneficiary Member States"[11]) in the Caribbean Region. This Assessment Report is for discussion and adoption by the HIPCAR Working Group on ICT Legislative Framework Meeting to be held in Saint Lucia on March 8-12, 2010.

The purpose of this Assessment Report is to provide an analysis of the key issues and common principles reflected in ICT regulatory and legislative frameworks relating to interception of communications in the Beneficiary Member States and to provide a reference document for policy makers, legislators and regulators in the Beneficiary Member States that will serve as a basis for harmonized policy guidelines to be developed in Phase II of the Work Plan, and that may be used to produce model legislation under Phase III of the Work Plan.

Section 3 of this Assessment Report briefly highlights the challenges inherent to legislating in the area of interception of communication, as well as the challenges posed by the task of harmonizing the legislative framework of interception in the Beneficiary Member States, given the varied legal and regulatory frameworks and the varied stages of development of ICT policy implementation and of interception of communications legislation.

Section 4 identifies the international and regional trends and best practices, which provide the basis for comparison with national laws, and eventual gap analysis.

Section 5 addresses an overview of current legislation in the Beneficiary Member States vis-à-vis the main issues associated with an effective legal framework for interception of communication.

Section 6 presents comparative law analysis based on international, regional, and national sceneries portrayed in Sections 4 and 5.

Section 7 shows tables picturing the current stage of legislative efforts in the Beneficiary Member Stages, including a matrix featuring main associated issues. Grades attributed to legislation of each individual Beneficiary Member State are rooted in the comments made in Sections 5 and 6.

Section 8 analyses main factors and criteria which may subsidy definition and implementation of policy guidelines.

Section 9 reproduces the text of some pieces of legislation of individual Beneficiary Member States.

Section 10 contains the bibliography researched as well as the sources of information considered in this Report.

---

[10] The full title of the HIPCAR Project is: "Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures". HIPCAR is part of a global ITU-EC-ACP project carried out with funding from the European Union set at EUR 8 million and a complement of USD 500,000 by the International Telecommunication Union (ITU). It is implemented by the ITU in collaboration with the Caribbean Telecommunications union (CTU) and with the involvement of other organizations in the region. (See www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html).

[11] Antigua and Barbuda, The Bahamas, Barbados, Jamaica, the Commonwealth of Dominica, the Domincan Republic,Haiti, Grenada, Guyana, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname and Trinidad and Tobago.

Section III: Challenges

Legislating on interception of communication is a task that presents several complex challenges, some of which result from increasing technological sophistication, while others relate to the difficulty of harmonizing different legal systems and national laws within a single region.

Cloud computing, re-mailing techniques, cryptography, and steganography, are examples of technological means which can be used by criminals and make hard or even unfeasible to intercept communication or to analyze it. Therefore, the use of such technologies for illicit purposes shall be a concern.

On the other hand, the required balance between interception requests and privacy rights is another challenge for implementing interception of communication as it may be subject to appraisal on a case-by-case basis in spite of the rapidly increasing volume of orders, some of them coming from different parts of the world.

Difficulties for implementing interception are also associated with complex management control. Huge amounts of accumulated data and multiple parameters for storage keeping and discard illustrate the point that intercepting communication is not only a legal matter, but also an administrative task.

Different legal systems to which Beneficiary Member States are affiliated, and different stages of development and implementation of their ICT policies, materialize additional complication for harmonizing national laws. Moreover, Beneficiary Member States have diverse legal and regulatory frameworks in their domestic environment.

Although Beneficiary Member States are parties to relevant regional and international conventions, and in most cases are members of the Caribbean Community, there is no Regional Sovereign power with authority to make laws on their behalf as a group and to ensure compliance, as is the case in the European Community.

To take the example of the OECS Member States, most of which are Beneficiary Member States of the HIPCAR Project, the Model Interception of Communications Act prepared by the OECS Legislative Drafting Facility in 2003 was approved by the Legal Affairs Committee, which comprises the Attorneys General (who are directly responsible for implementing the policy on interception), in that same year, for enactment in all the OECS Member States, however, to date, only Saint Lucia has enacted an Interception of Communications Act (followed by similar law in Jamaica).

For more complete reference on challenges affecting interception of communication, the reading of Sections 3.2 and 3.3 of ITU's document named "Understanding Cybercrime: a Guide for Developing Countries"[12] is recommended.

[12] Available at www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf.

Section IV: International and Regional Trends and Best Practices

As interception of communication poses various, important challenges to overcome, there is substantive panorama of international and regional trends and best practices which have focused in its regulation. These legislative experiences and recommendations have improved throughout time and now form a set of benchmark samples worth quoting[13]:

4.1 Council of Europe's Budapest Convention on Cybercrime

Article 20 – Real-time collection of traffic data

(1) Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a. collect or record through the application of technical means on the territory of that Party, and
b. compel a service provider, within its existing technical capability:
    i. to collect or record through the application of technical means on the territory of that Party; or
    ii. to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

(2) Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

(3) Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

(4) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

(1) Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a. collect or record through the application of technical means on the territory of that Party, and
b. compel a service provider, within its existing technical capability:
    i. to collect or record through the application of technical means on the territory of that Party, or

[13] For more complete reference, see items 6.2.8 through 6.3 of ITU's document "Understanding Cybercrime: a Guide for Developing Countries" (at www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf).

ii. to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

(2) Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

(3) Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

(4) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

4.2 Commonwealth Computer and Computer Related Crimes Model Law [14]:

Interception of electronic communications

18.(1) If a **[*magistrate*] [*judge*]** is satisfied on the basis of [***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 magistrate [***may***] [***shall***]:

a. 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

b. authorize a police officer to collect or record that data through application of technical means.

Interception of traffic data

19.(1) If a police officer is satisfied that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the police officer 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 a specified police officer to collect or record that data.

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

[14] Availabe at www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf.

Section IV

4.3 ITU's Constitution [15]:

Article 37:

1. Member States agree to take all possible measures, compatible with the system of telecommunications used with a view to ensuring the secrecy of international correspondence.

2. Nevertheless, they reserve the right to communicate such correspondence to the competent authorities in order to ensure the application of their national laws or the execution of international conventions to which they are parties.

4.4 International Standards:

There are international standards which acknowledge generally recognized best practices in the monitoring of electronic communications. ISO 27000 norms on Information Security, as well as ISO 38500 norms on IT Governance, are examples of such non-binding norms[16]. There are joint initiatives in course putting different organisations together towards improving techniques of identification and automatic capture of data and of information technology security, including ISO, ITU and CEI[17].

4.5 European Convention on Human Rights for the Protection of Human Rights and Fundamental Freedoms(ECHR) [18]:

Article 8:

"1. Everyone has the right to respect for his ... correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedom of others.".

Article 8 has been used as the basis for legality of national legal procedures for interception of communications by Officials, for example in the Klass Case[19] and to force European states to introduce a legal procedure, for example in the Malone Case[20] in the United Kingdom.

4.6 Universal Declaration of Human Rights:

Article 12:

"No one shall be subjected to arbitrary interference with his privacy, or correspondence, everyone has the right to the protection of the law against such interference.

---

15 www.itu.int/net/about/basic-texts/constitution/chaptervi.aspx.

16 Which, however, may be translated and incorporated into national legislation by means of their inclusion in the local normalisation system, which is usually regulated by statutory law.

17 See "La criminalité numérique", Institut Nacional des Hautes Études de Securité, Cahiers de la Securité, n. 6, Paris, oct-dec. 2008, p.157).

18 The convention is available at www.hrcr.org/docs/Eur_conveniton/euroconv3.html.

19 4 Klass v Germany [1978] 2 EHRR 214

20 Malone v UK [1984] 7 EHRR 14.

4.7 Commonwealth Computer and Computer Related Crimes Model Law [21]:

(8) A person who intentionally without lawful excuse or jurisdiction intercepts by technical means:

a. non- public transmission from within a computer system; or

b. electronic magnetic emissions for a computer system that are carrying computer data,

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

It shall be noted that Commonwealth's 2nd Meeting of Expert group on Computer and Computer-related Crime which convened in 2002 has recommended that the model law be redrafted and that section 8 should be framed in broader terms to capture interception of communications that was non-public regardless of whether the media used was private or public.

4.8 OECD Guidelines [22]

Recommendation 5:

"The fundamental rights of individuals to privacy, including secrecy of communications, should be respected in national cryptographic policies and in the implementation and use of cryptographic methods.".

4.9 Council of Europe Data Protection Convention:

Article 7 of the Council of Europe's Data Protection Convention[23] requires that appropriate security measures shall be taken for the protection of personal data against unauthorized access or dissemination. And Recommendation R (95)13 of the Committee of Ministers (adopted on September 11, 1995) "concerning criminal procedural law connected with information technology" made the recommendations that criminal laws should be modified to allow interception in the investigation of serious offences against telecommunications or computer systems and that measures should be considered to minimize the negative effects of cryptography without affecting its use more than is strictly necessary.

4.10 EU Data Protection Directive 95/46/EC

The European Union's Directive 95/46EC is primarily concerned with the protection of data stored in databases and is of indirect relevance to interception of communications only . The Preamble includes the following provision:

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

and Article 1 of the Directive states the following as the object of the Directive:

---

21 Availabe at www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf.

22 Recommendation of the OECD Council concerning Guidelines for the Security of Information Systems, adopted on November 26-27 1993 C(92) 188/Final.

23 Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data 1981.

"In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.".

Article 2(h) of the Directive specifies that user consent must be "freely given specific and informed". Further, Article 24 of the Data Protection Directive requires Member States to establish appropriate sanctions in case of infringements and Article 28 says that independent authorities must be charged with supervising implementation. These provisions of the Data Protection Directive also apply in the area of confidentiality of communications.

4.11 EU Directive 97/66/EC

European Union's Directive 97/66EC, in its preamble, makes it clear that the Directive does not address the protection of fundamental rights and freedoms related to activities which are not governed by Community law. Furthermore, it does not affect the right of Member States to take such measures as they consider necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. However, Article 5 states that Member States shall ensure via national regulations the confidentiality of communications by means of a public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorized.

4.12 EU Directive 2002/58/EC

Article 5 of the EU Directive 2002/58/EC on privacy and electronic communications requires EU Member States to ensure confidentiality of communications and related traffic data by enacting national legislation to prohibit unlawful interception and surveillance unless the users concerned have consented to this.

Article 6 of the EU Directive 2002/58/EC provides for traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service to be erased or made anonymous when it is no longer needed for the purpose of the transmission.

By virtue of Article 15 of the EU Directive 2002/58/EC, Member States are given the discretion to adopt legislative measures to restrict the scope of the rights and obligations provided for in, among others, articles 5 and 6.

4.13 Organisation of Eastern Caribbean States:

The Organisation of Eastern Caribbean States, in providing model legislation for its Member States and having regard to Constitutional limitations of its Member States, has issued the following guidelines to be considered before a decision is taken to intercept any communication:

- that the public interest which will be served by obtaining the information which it is hoped will result from the interception of communications is of sufficient importance to justify such interception;
- that if the interception is granted, it will offer reasonable prospects of providing the information sought;
- that the other methods of obtaining the information such as surveillance or the use of informants have been tried or failed or from the nature of the case is not feasible;
- that the interception should cease as soon as the information is provided of the kind sought or it has become apparent that it is unlikely to provide it;

- that the products of the interception not directly relevant to the purpose receive no wider circulation than is essential for carrying it out[24].

In addition to international and regional legislation and best practices, there are some countries'national legal instruments and best practices which are worth mentioning:

4.14 Australia

The Telecommunications (Interception and Access) Act 1979 (TIA Act) of Australia gives legislative effect to the policy of the Australian Government on interception of and access to communications.

The main purpose of the TIA Act is to protect the privacy of individuals using the telecommunications system of Australia by making it an offence to intercept communications passing over that system other than in accordance with the provisions of the Interception Act and to specify the circumstances in which it is lawful for interception to take place.[25]

A prohibition is placed by the TIA Act on the interception of communications which passes over a telecommunications system and on access to stored communications, including voice mail messages, SMS and emails that are stored on a carrier's equipment, except where it is authorized in circumstances that are specified. The main exception to the prohibition is to enable law enforcement agencies, in specific circumstances, to lawfully access or intercept telecommunications pursuant to an interception warrant or a stored communications warrant issued under the TIA Act. Other exceptions are specified for a small number of particular purposes including the maintenance and operation of a telecommunications system and tracing the location of callers in emergencies.

Since 13 June 2006, the TIA Act applies to stored communications including voice messages, SMS and e-mail stored on carriers' equipment. At that time also, the name of the Act was changed to the Telecommunications (Interception and Access) (Amendment) Act 2006 (the 2006 Act). The 2006 Act provides a regime for governing access to stored communications held by a telecommunications carrier, establishes a new "stored communications warrant" and makes numerous other changes to the pre-existing interception provisions of the Act.

The Explanatory Memorandum to the 2006 Act[26] states that: *"In relation to both telecommunications interception and access to stored communications, the Act makes clear that the general position is that these activities are prohibited, except in certain clearly defined situations. This reflects the primary focus of the Act which is to protect the privacy of communications.".*

The provisions of the TIA Act relating to stored communications apply to communications such as email, SMS and voice mail messages that either have not commenced, or have completed, passing over a telecommunications system, and that are stored on a telecommunications carrier's equipment (including on an Internet Service Provider's equipment). [27]

The provisions of the TIA Act relating to interception apply to communications that are "passing over a telecommunications system", that is, "live" or "real-time" communications such as telephone call conversations and communications in transit over the Internet including while passing through ISPs' equipment such as routers, etc[28].

---

24 Notes on OECS Interception of Communications Bill, page 7, available at http://unpan1.un.org/intradoc/groups/public/documents/TASF/UNPAN024635.pdf

25 TI Act Annual Report 2004.

26 www.comlaw.gov.au/comlaw/legislation/bills1.nsf/0/816D9E25E76473B1CA2571180012980D/%24file/06010EM.pdf at page

27 www.efa.org.au/Issues/Privacy/tia.html

28 www.efa.org.au/Issues/Privacy/tia.html

A number of accountability, controls and safeguard mechanisms involving record keeping, reporting, restrictions on use of intercepted or accessed information, are contained in the TIA Act

In 1997, Australia passed the *Telecommunications Act 1997,* requiring carriers and carriage service providers (telecommunications service providers) to comply with obligations concerning an interception capability and special assistance capability. The TIA Act is technology neutral. It applies to all telecommunications including the Internet. Under the TIA Act, carriers bear the majority of the capital and ongoing costs for developing and maintaining interception capability.[29]

In 2009, the Australian Government approved the release of exposure draft legislation to facilitate public consultation on proposed reforms to the TIA Act. The policy proposal developed by the Attorney General's' Department was set out in the draft TIA (Amendment) Bill 2009 which is aimed at improving the capacity of owners and operators of computer networks to undertake activities to protect their networks. Such Amendment Bill has recently passed the Senate[30].

4.15 United States of America

While interception is defined in the Title 18 of the US Code, the interception of communications policy in the United States of America (USA) is covered by two main laws namely the 1968 Title III of the Omnibus Crime Control and Safe Streets Act[31], and the 1978 Foreign Intelligence Surveillance Act[32] (FISA) which governs wiretapping for intelligence purposes where the subject of the investigation must be a non-US national or a person working as an agent on behalf of a foreign country. The US Congress passed the Communications Assistance for Law Enforcement Act (CALEA) in 1994[33]. The purpose of the CALEA is stated as follows:

"To amend title 18, United States Code, to make clear a telecommunications carrier's duty to cooperate in the interception of communications for Law Enforcement purposes, and for other purposes.".

The CALEA was enacted by the U.S. Congress to assist law enforcement and the Federal Bureau of Investigation (FBI) to carry out wiretap operations more effectively having regard to the emerging digital voice and wireless networks at the time. This Act provides broad guidelines to network operators on how to assist law enforcement agencies in setting up interceptions and the types of data to be delivered. The CALEA obliges telecommunications companies to make it possible for law enforcement agencies to tap any phone conversations carried out over its networks, as well as making call detail records available. The CALEA stipulates that it must not be possible for a person to detect that his or her conversation is being monitored by the respective government agency. The US Federal Communications Commission (FCC) has mandated that CALEA is extended to include interception of publicly-available broadband networks and Voice over IP services that are interconnected to the Public Switched Telephone Network (PSTN)[34].

In response to the 9/11 Terrorist events, the US Congress incorporated provisions related to enhanced electronic surveillance in the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (USA Patriot Act). The wiretap provisions in the USA Patriot Act are updates to the provisions expressed under the FISA law.

---

29 www.publicsafety.gc.ca/media/bk/2005/bk20051115

30 See at www.cio.com.au/article/334902/telecommunications_amendment_bill_passes.

31 The Omnibus Crime Control and Safe Streets Act of 1968 (Pub.L. 90-351, June 19 1968, 82 Stat. 197, 42 U.S.C. § 3711) was legislation passed by Congress that established the Law Enforcement Assistance Administration (LEAA). Title III of the Act set rules for obtaining wiretap orders in the United States.

32 "Foreign Intelligence Surveillance Act" 2006. October 16 2009 www.bookrags.com/wiki/Foreign_Intelligence_Surveillance_Act.

33 is a United States wiretapping law passed in 1994 (Pub. L. No. 103-414, 108 Stat. 4279).

34 http://en.wikipedia.org/wiki/Communications_Assistance_for_Law_Enforcement_Act#Provisions_of_CALEA.

4.16 United Kingdom

Interception of communications is a long established government practice in the United Kingdom, for which there was no comprehensive legislative framework until 1985, when the Interception of Communications Act (IOCA) was enacted. The IOCA was prompted by the Malone Case[35] and provided a legislative framework for interception of communications sent by post through a telecommunications system with a warrant system together with internal safeguards, monitoring and complaints mechanisms and created an offence of unlawful interception of communications.[36]

The huge changes in the telecommunications and postal market, and the wide expansion in the nature and range of services available gave rise to concerns that were beyond the scope of the IOCA. As illustrated in the Home Office Consultation Paper on Interception published in 1999 criminals including terrorists have been quick to exploit these extraordinary changes[37] and recognising the need for new legislation, the United Kingdom repealed the IOCA and replaced it with the Regulation of Investigatory Powers Act 2000 (RIPA) which establishes a regulatory framework relating to certain investigatory powers. The RIPA was enacted in the United Kingdom in to incorporate the ECHR into national law, in particular Article 8. The RIPA provides a regime for the interception of communications and goes beyond what is required for human rights purposes and provides also for the changed nature of the communications industry since 1985. The RIPA provisions also implement Article 5 of Council Directive 97/66EC of 15 December 1997, (the Telecommunications Data Protection Directive), which requires Member States to safeguard the confidentiality of communications.

The purpose of the RIPA is to ensure that the investigatory powers are exercised lawfully and in accordance with human rights and in particular in accordance with the ECHR. In particular, the RIPA requires that persons authorizing the use of covert techniques give proper consideration to whether the use of investigatory powers are necessary and proportionate.

The following areas are regulated by the RIPA:

- The interception of communications (for instance, the content of telephone calls, e-mails or postal letters).
- The acquisition and disclosure of communications data (information from communications service providers relating to communications).
- The carrying out of covert surveillance:
  - in private premises or vehicles (‘intrusive surveillance’) or
  - in public places but likely to obtain private information about a particular person (‘directed surveillance’).
- The use of covert human intelligence sources (such as informants or undercover officers)
- Access to electronic data protected by encryption or passwords.
- RIPA also provides a number of important safeguards:
- It strictly limits the people who can lawfully use covert techniques, the purposes for and conditions in which they can be used and how the material obtained must be handled
- It reserves the more intrusive techniques for intelligence and law enforcement agencies acting against only the most serious crimes, including in the interests of national security

---

35 Ibid 15.

36 See Home Office (1999) Interception of Communications A consultation Paper. Available from www.homeoffice.gov.uk/documents/cons-1999-interception-comms2835.pdf?view=Binary.

37 Ibid 22.

- It provides for the appointment of independent oversight Commissioners and the establishment of an independent tribunal to hear complaints from individuals who believe the techniques have been used inappropriately.[38]

However, the European Commission appears to have concerns over the adequacy of the provisions of the RIPA and on October 30, 2009 the following article was published by European Commission in Brussels on October 29, 2009:

Telecoms: Commission steps up UK legal action over privacy and personal data protection

The Commission today moved to the second phase of an infringement proceeding over the UK to provide its citizens with the full protection of EU rules on privacy and personal data protection when using electronic communications. European laws state that EU countries must ensure the confidentiality of people's electronic communications like email or internet browsing by prohibiting their unlawful interception and surveillance without the user's consent. As these rules have not been fully put in place in the national law of the UK, the Commission today said that it will send the UK a reasoned opinion.

"People's privacy and the integrity of their personal data in the digital world is not only an important matter, it is a fundamental right, protected by European law. That is why the Commission is vigilant in ensuring that EU rules and rights are put in place," said EU Telecoms Commissioner Viviane Reding. "Ensuring digital privacy is a key for building trust in the internet. I therefore call on the UK authorities to change their national laws to ensure that British citizens fully benefit from the safeguards set out in EU law concerning confidentiality of electronic communications."

The Commission maintains its position that the UK is failing to comply with EU rules protecting the confidentiality of electronic communications like email or surfing the internet, which are provided in the ePrivacy Directive 2002/58/EC and the Data Protection Directive 95/46/EC. This follows a thorough analysis of the UK authorities' response to the letter of formal notice – the first phase in an infringement proceeding – sent to them by the Commission on 14 April 2009 (IP/09/570). The Commission launched this legal action following its inquiry into the response given by the UK authorities to UK citizens' complaints about the use of behavioural advertising by internet service providers.

Specifically, the Commission has identified three gaps in the existing UK rules governing the confidentiality of electronic communications:

- *There is no independent national authority to supervise interception of communications, although the establishment of such authority is required under the ePrivacy and Data Protection Directives, in particular to hear complaints regarding interception of communications.*
- *The current UK law – the Regulation of Investigatory Powers Act 2000 (RIPA) – authorizes interception of communications not only where the persons concerned have consented to interception but also when the person intercepting the communications has 'reasonable grounds for believing' that consent to do so has been given. These UK law provisions do not comply with EU rules defining consent as freely given specific and informed indication of a person's wishes.*
- *The RIPA provisions prohibiting and providing sanctions in case of unlawful interception are limited to 'intentional' interception only, whereas the EU law requires Members States to prohibit and to ensure sanctions against any unlawful interception regardless of whether committed intentionally or not.*

The UK has two months to reply to this second stage of the infringement proceeding. If the Commission receives no reply, or if the response presented by the UK is not satisfactory, the Commission may refer the case to the European Court of Justice.

---

[38] http://security.homeoffice.gov.uk/ripa/about-ripa/

4.17 Germany

The German Constitutional Court has issued important decisions[39] on the theme of interception of communication, for instance, on the inconstitutionality of state laws, such as the ones relating to the states of Niedersachsen and of Thuringen, conditioning the interception of telephone communication, including collection of traffic data, location data, electronic mail, and electronic short messages, to specific suspicion.

[39] Available at www.bundesverfassungsgericht.de/entscheidungen/rs20050727_1bvr0.

Section V: Overview of the Countries and Their Legal Instruments

Although provision is made under the Telecommunications Act of some of the Beneficiary Member States[40] and in cyber-security legislation in other Beneficiary Member States for the prohibition of any interception of telecommunications which may transmit, emit, or receive public telecommunications without the approval of the competent authority appointed pursuant to the Act, to date only two beneficiary States, namely Jamaica and Saint Lucia are reported to have substantial legislation specifically relating to implementing lawful interception of communication. Those cases are described below, followed by a table including the specific situation of each Beneficiary Member State in the light of the main issues affecting interception of communication.

Jamaica

Jamaica has enacted the Interception of Communications Act in 2002[41], amended the Act in 2005[42] and in 2006, and a Cybercrime Act has passed the Senate in December 2009.

The Jamaica Interception of Communications Act prohibits unlawful interception and provides for the lawful interception of communications by an authorized officer where the communication is intercepted in obedience to a warrant issued by a Judge in Chambers, where the person intercepting has reasonable grounds for believing that the person to whom or by whom the communication is transmitted consents to the interception; the communication is intercepted as an ordinary incident to the provision of telecommunications services or to the enforcement of any enactment relating to the use of those services; the communication is not a private communication; the communication is stored communication and is acquired in accordance with the provisions of any other law; or the interception is of a communication transmitted by a network that is not a public telecommunications network and is done by a person who has a right to control the operation or use of the network or has the expressed consent of the person by whom or to whom the communication is transmitted.

A warrant will not be issued unless the Judge is satisfied that the warrant is necessary in the interests of national security or for the prevention or detection of an offence of kidnapping or abduction, money laundering, producing. manufacturing, supplying or otherwise dealing in any dangerous drug, murder or treason, transporting or storing a dangerous drug where possession of such drug, importation exportation or transshipment of any firearm or ammunition, manufacture of or dealing in firearms or ammunition, illegal possession of a prohibited weapon or any other firearm or ammunition, corruption or arson.

Amendments made to the Interception of Communications Act in Jamaica after its enactment allow law enforcement officials to intercept the communication of suspected criminal offenders, without a court order, for a period of up to seven days. During the Parliamentary debate regarding the amendments the then leader of Government Business and Minister for National Security, Dr. Peter Phillips informed the House that the changes to the Act were occasioned "primarily by (the) technological changes that have occurred subsequent to the original legislation coming into effect". He explained that the effort "is to facilitate law enforcement agencies in securing the original purposes of the Act, in light of these changes that have occurred to the technologies since the original Bill was passed in 2002". The Minister noted

---

40 For Telecommunications Act – Suriname and ECTEL Member States of Commonwealth of Dominica, Grenada, Saint Kitts and Nevis, Saint Lucia and Saint Vincent and the Grenadines and for cybersecurity legislation – Jamaica and Saint Vincent and the Grenadines.

41 Act No. 5 of 2002.

42 Act No. 18 of 2005.

further, that the revised Bill sought to "allow service providers to maintain the appropriate facilities, and secondly, to enable law enforcement to deal with the technological changes which allow for a rapid change of instruments, for the non-permanence of instruments and for other necessary assistance to be given to law enforcement".

The list of offences in the Act were extended to include the sale and trafficking of children, defilement by threats or fraud, forcible abduction, administering drugs, child stealing, aiding and abetting or conspiring to commit any of the scheduled offences. While the primary intention of the Act – to curb criminal activity – found favour with members of the Opposition, they raised concerns about the infringement of individual rights. The Opposition Spokesman on National Security and Leader of Opposition Business, Derrick Smith at the time said that while the Opposition agreed with elements of the Act, "in the interest of national security", if credible information came to them over time, "we will not be reluctant or hesitate to rescind what we are agreeing to do today, because we are overly concerned about the rights of individuals in this country". "We hope this amendment will improve the investigative skills of the members of the security forces and we hope in due course, it will help to bring some of these criminals, locally and overseas, to book," he added.

Saint Lucia

In 2004, the Organization of Eastern Caribbean States (OECS), through the OECS Legislative Drafting Facility, was given a mandate by the Legal Affairs Committee to prepare draft model legislation on interception of communications. Although the Draft Model Interception of Communications Bill was approved by the Legal Affair Committee for enactment in all OECS Member States, Saint Lucia is the only OECS Member State to enact a revised version of the harmonized Interception of Communications legislation, in 2005[43].

The Interception of Communications Act was passed in Saint Lucia with the support of the Parliamentary Opposition. The Act allows an authorized officer to make an application to a High Court Judge for permission to intercept the communications of a person or persons involved in serious criminal activity including murder; drug trafficking, money laundering and kidnapping. Provisions is made in the Act for safeguards against abuse, including adjudication by an Appeals Tribunal with appeals against the appeals Tribunal's decisions going to the Court of Appeal and the prescribing of a Code of Conduct by the Chief Justice for officers who will be authorized with enforcement powers under the Act.

The law allowing for legal interception of communications of criminals in Saint Lucia is regarded as a necessary and vital tool in the fight against those engaged in the use of technology to facilitate serious criminal activity. The legislation is aimed not at invasion of privacy of individuals or at depriving or restricting the rights of individuals but rather at enhancing the capability of the local law enforcement agencies to intercept, prevent or reduce crime where possible. The interception of communication may only take place when the information cannot reasonably acquired by any other means and interception direction and entry warrant is authorized by a judge and only when a judge is satisfied that it is absolutely necessary. The in-built safeguards in the legislation are intended to protect the rights of innocent persons and reduce the possibility of abuse by those administering the law[44].

Panorama of Beneficiary Member States' Legislation Vis-à-vis Key Issues

For clearer identification on the different approaches taken by Beneficiary Member States in regulating interception of communication, their legislation is commented in the paragraphs to follow vis-à-vis key issues associated, which include:

- Policy framework for interception.

---

43 Act No. 31 of 2005, Now Cap. Revised Laws of Saint Lucia.

44 See www.stlucia.gov.lc/gis/nationwide/2005/NationWide05November2005.pdf

Section V

- Institutional framework required for interception capabilities.
- Definition of interception.
- Scope of the right to intercept.
- Performance of Interception.
- Confidentiality measures.
- Monitoring measures.
- Interception capabilities.
- Internal safeguard measures.
- Dispute resolution.

5.1 Policy Framework for Interception

- There is a legal mandate/law to in place to support or address interception of communications.
- The law gives legislative effect to clear policy guidelines.
- The law reflects common key principles that are in line with international best practices and international and regional obligations.

Antigua and Barbuda – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

The Bahamas – NONE

Barbados – NONE

Belize – NONE

Dominica – LIMITED
Limited, legislative framework proposed based on OECS Model and EUSFA Review. The Bill tabled in Parliament in September 2009.

Dominican Republic – NONE

Grenada – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill .

Guyana – NONE

Haiti – NONE

Jamaica – GOOD

Interception of Communications Act, No. 5 of 2002 and No. 18 of 2006

The Act came into force on 15th March 2002 and was amended in 2006.

St. Kitts and Nevis – LIMITED

Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Saint Lucia – GOOD

Section V

Interception of Communications Act, Cap. 3.12.

The Act was based on the OECS Harmonised draft Interception of Communications Bill.

The Act came into force on 14th August 2006.

The Preamble to the Act states that it is: An Act to provide for the interception of communications and the provision of information relating to interception in Saint Lucia and for related matters.

St. Vincent and the Grenadines – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Suriname – NONE

Trinidad and Tobago – NONE

5.2 Institutional Framework Required for Interception Capabilities

- There is a relevant government department, agency or regulator responsible for implementing or administering the law.
- There is an authority responsible for authorizing interception of communications.

Antigua and Barbuda – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

The Bahamas – NONE

Barbados – NONE

Belize – NONE

Dominica – LIMITED
*Limited, legislative framework proposed based on OECS Model and EUSFA Review. Bill in Parliament as at September 2009.

Dominican Republic – NONE

Grenada – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Guyana – NONE

Haiti – NONE

Jamaica – GOOD

Interception of Communications Act, No. 5 of 2002 and No. 18 of 2006

Section 2 – "authorized officer" means-
a. the Commissioner of Police;

b. the officer of the Jamaica Constabulary Force in charge of-
   i. internal security; or
   ii. the National Firearm and Drug Intelligence Centre or any organization replacing the same; or
c. the Chief of Staff, or the head of the Military Intelligence Unit, of the Jamaica Defence Force;

Section 4 –. Subject to the provisions of this section, an authorized officer may apply ex parte to a Judge in Chambers for a warrant authorizing the person named in the warrant-
a. to intercept, in the course of their transmission by means of a public or private telecommunications network, such communications as are described in the warrant; and
b. to disclose the intercepted communication to such persons and in such manner as may be specified in the warrant.

St. Kitts and Nevis – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Saint Lucia – GOOD

Interception of Communications Act, Cap. 3.12.

Section 2 –

"**authorised officer**" means–
a. the Commissioner of Police;
b. the Director of the Financial Intelligence Authority;
c. the Comptroller of Customs;
d. a person for the time being lawfully exercising the functions of a person stated in paragraphs (a) to (c);
e. a person authorised in writing to act on behalf of a person mentioned in paragraphs (a) to (c).

"**Minister**" means the Minister responsible for national security.

Section 4 An authorised officer who wishes to obtain an interception direction under the provisions of this Act shall request the Attorney General or the Director of Public Prosecutions to make an application ex parte to a judge in chambers on his or her behalf.

St. Vincent and the Grenadines – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Suriname – NONE

Trinidad and Tobago – NONE

5.3 Definition of Interception

- The definition of interception provided in the legislative framework.
- The definition of interception is technology neutral and not confined to any particular communication handling system.

- The definition is broad enough to cover communications sent via various types of networks, e-mail systems and other wireless transmissions.

Antigua and Barbuda – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

The Bahamas – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Barbados – NONE

Belize – NONE

Dominica – LIMITED
*Limited, legislative framework proposed based on OECS Model and EUSFA Review. Bill in Parliament as at September 2009.

Dominican Republic – NONE

Grenada – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Guyana – NONE

Haiti – NONE

Jamaica – GOOD

Interception of Communications Act, No. 5 of 2002 and No. 18 of 2006

Section 2(1)"intercept" in relation to a communication means the-

a. monitoring of transmissions made by wireless telegraphy to or from apparatus comprising in the network;
b. monitoring or modification of, or interference with, the network by means of which the communication is transmitted, so as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication, and "interception" shall be construed accordingly;

St. Kitts and Nevis – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Saint Lucia – GOOD

Interception of Communications Act, Cap. 3.12.

Section 2 – "**intercept**" includes–

a. aural or other acquisition of the contents of a communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication;
b. monitoring a communication by means of a monitoring device;
c. viewing, examining, or inspecting the contents of a communication; and
d. diverting of any communication from its intended destination to any other destination;

and "interception" shall be construed accordingly;

Section V

"**intercepted communication**" means a communication which during the course of its transmission by means of a postal service or a telecommunication network is intercepted;

St. Vincent and the Grenadines – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Suriname – NONE

Trinidad and Tobago – NONE

5.4 Scope of the Right to Intercept

- The law provides a framework for authorizing interception of communications which allows for public confidence.
- Unauthorized interception to communications is criminalized in the law.
- The punishment provided in the law is appropriate.

Antigua and Barbuda – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

The Bahamas – NONE

Barbados – NONE

Belize – NONE

Dominica – FAIR
*Fair, legislative framework proposed in the OECS Interception of Communications Bill.

Dominican Republic – NONE

Grenada – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Guyana – NONE

Haiti – NONE

Jamaica – GOOD

Interception of Communications Act, No. 5 of 2002 and No. 18 of 2006

3.(1)Except as provided in this section, a person who intentionally intercepts a communication in the course of its transmission by means of a telecommunications network commits an offence and is liable upon summary conviction in a Resident Magistrate's Court to imprisonment for a term not exceeding three years or to a fine not exceeding three million dollars or to both such fine and imprisonment.

(2) A person does not commit an offence under this section if-

a. the communication is intercepted in obedience to a warrant issued by a Judge under section 4;
b. he has reasonable grounds for believing that the person to whom or by whom the communication is transmitted consents to the interception;

c. the communication is intercepted as an ordinary incident to the provision of telecommunications services or to the enforcement of any enactment relating to the use of those services;
d. the communication is not a private communication;
e. the communication is a stored communication and is acquired in accordance with the provisions of any other law; or
f. the interception is of a communication transmitted by a network that is not a public telecommunications network and is done by a person who has-
   i. a right to control the operation or use of the network; or
   ii. the express or implied consent of a person referred to in sub-paragraph (i).

(3) The court by which a person is convicted of an offence under this section may order that any device used to intercept a communication in the commission of the offence shall be forfeited and disposed of as the court may think fit.

(4) For the purposes of subsection (I), a communication shall be taken to be in the course of transmission by means of a telecommunications network at any time when the network by means of which the communication is being or has been transmitted is used for storing the communication in a manner that enables the intended recipient to collect it or otherwise have access to it.

St. Kitts and Nevis – LIMITED

*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Saint Lucia – GOOD

Interception of Communications Act, Cap. 3.12.

Prohibition of interception

(1) Except as provided in this section, a person who intentionally intercepts a communication in the course of its transmission by means of a public postal service or a telecommunications network commits an offence, and on conviction on indictment, is liable to a fine not exceeding $20,000 or a term of imprisonment not exceeding 4 years, or to both.

(2) A person does not commit an offence under subsection (1) if–
a. the communication is intercepted in accordance with an interception direction issued under section 5 or 10 or an entry warrant issued under section 8 or 10;
b. subject to subsection (3), that person has reasonable grounds for believing that the person to whom or by whom the communication is transmitted consents to the interception;
c. the communication is stored communication and is acquired in accordance with the provisions of any other law;
d. the communication is intercepted as an ordinary incident to the provision of public postal services or telecommunications services or to the enforcement of any law in force in Saint Lucia relating to the use of those services;
e. the interception is of a communication made through a telecommunications network that is so configured as to render the communication readily accessible to the general public; or
f. the interception is of a communication transmitted by a private telecommunications network and is done by a person who has–
   i. a right to control the operation or use of the private telecommunications network, or
   ii. the express or implied consent of a person referred to in subparagraph (i).

(3) A person does not commit an offence under subsection (1) where–
a. the communication is one sent by or intended for a person who has consented to the interception; and

Section V

b. the person is an authorised officer who believes that the interception of communication is necessary for the purpose of an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health or in the interests of national security.

(4) A court convicting a person of an offence under this section may, in addition to any penalty which it imposes in respect of the offence, order the forfeiture and disposal of any device used to intercept a communication in the commission of the offence.

(5) For the purposes of this section, a communication shall be taken to be in the course of transmission by means of a telecommunications network at any time when the network by means of which the communication is being or has been transmitted is used for storing the communication in a manner that enables the intended recipient to collect it or otherwise have access to it.

St. Vincent and the Grenadines – FAIR
*Fair, legislative framework proposed in the OECS Interception of Communications Bill.

Suriname – NONE

Trinidad and Tobago – NONE

5.5 Interception Approval

- The law provides grounds for authorizing interception.
- Provision is made in the law for authorization of the person executing the interception.
- The scope of interception authorisation is specified in the law.
- The legislative framework provides for expiry of an interception authorization.
- The powers of an interception authorisation is specified in the law.
- Provision is made in the law for the person executing the interception direction or warrant to be assisted by any other person.

Antigua and Barbuda – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

The Bahamas – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Barbados – NONE

Belize – NONE

Dominica – LIMITED
*Limited, legislative framework proposed based on OECS Model and EUSFA Review. Bill in Parliament as at September 2009.

Dominican Republic – NONE

Grenada – LIMITED

*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Guyana – NONE

Haiti – NONE

Jamaica – GOOD

Interception of Communications Act, No. 5 of 2002 and No. 18 of 2006

St. Kitts and Nevis – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Saint Lucia – GOOD

Interception of Communications Act, Cap. 3.12.

8.(1) An entry warrant shall not be issued by a judge unless there exists with respect to the premises to which the application for an entry warrant relates, a related interception direction.

(2) Where the Attorney General or the Director of Public Prosecutions–

a. makes an application for an interception direction on behalf of an authorised officer under section 4, the Attorney General or the Director of Public Prosecutions may at the time of making the application, also apply to the judge for the issuance of an entry warrant with respect to the premises to which the interception direction relates; or
b. made an application for an interception direction on behalf of an authorised officer under section 4, and the authorised officer on whose behalf the application was made, is not available, any other authorised officer may, at any such stage after the issuance of the interception direction in respect of which such an application was made, but before the expiry of the period or the extended period for which it has been issued, request the Attorney General or the Director of Public Prosecutions to apply ex parte to a judge for the issuance of an entry warrant with respect to the premises to which the interception direction relates.

(3) Subject to section 9, an application for an entry warrant referred to in subsection (2), shall be in writing and in the prescribed form and shall–

a. be accompanied by an affidavit deposing the–
   i. name of the authorised officer on behalf of which the application is made,
   ii. premises in respect of which the entry warrant is required, and
   iii. the specific purpose for which the application is made;
b. if the application is made in terms of subsection (2)(b), also contain proof that an interception direction has been issued, and an affidavit setting forth the results, if any, obtained in the interception direction concerned from the date of its issuance up to the date on which the application was made, or a reasonable explanation of the failure to obtain such results; and
c. indicate whether any previous application has been made for the issuing of an entry warrant for the same purpose or in respect of the same premises specified in the application and, if such previous application exists, indicate the status of the previous application.

(4) Subject to subsections (1) and (5), a judge may upon an application made to him or her by the Attorney General or the Director of Public Prosecutions on behalf of an authorised officer, issue an entry warrant.

(5) An entry warrant shall be issued if the judge is satisfied, on the facts alleged in the application concerned that–

a. the entry into the premises is necessary for the purpose–
   i. of intercepting a postal article or a communication on the premises,
   ii. for installing and maintaining an interception device on, or
   iii. for removing an interception device from, the premises; and
b. there are reasonable grounds to believe that it would be impracticable to intercept a communication under the interception direction concerned otherwise than by the use of an interception device installed on the premises.

(6) An entry warrant–
a. shall be in the prescribed form in writing;
b. shall contain the information referred to in subsection (3)(a)(ii) and (iii); and
c. may contain conditions or restrictions relating to the entry upon the premises concerned as the judge may consider necessary.

(7) An entry warrant shall permit an authorised officer to enter upon the premises specified in the entry warrant for the purposes of–
a. intercepting a postal article or a communication by means of an interception device;
b. installing and maintaining an interception device; or
c. removing an interception device.

(8) An entry warrant shall expire when whichever of the following occurs first–
a. the period or the extended period for which the related interception direction concerned has been issued lapses;
b. it is terminated under section 10 by a judge; or
c. the interception direction to which it relates is terminated in accordance with section 9 or 10.

(9) When an entry warrant has expired under subsection (8)(a), the authorised officer on whose behalf the application was made or, if he or she is not available, any other authorised officer who would have been entitled to request the Attorney General or the Director of Public Prosecutions to make the application, shall, as soon as practicable after the date of expiry of the entry warrant, and without applying to a judge for the issuing of a further entry warrant, remove, or cause to be removed, any interception device which has been installed and which, at the expiry date of the entry warrant, has not yet been removed from the premises concerned.

14. Execution of interception direction or entry warrant

(1) If an interception direction or an entry warrant or both, has been issued under the provisions of this Act, an authorised officer may execute that interception direction or entry warrant or both.

(2) An authorised officer who executes an interception direction or an entry warrant or assists with the execution thereof may intercept, at any place in Saint Lucia, any communication in the course of its transmission to which the interception direction applies.

(3) Where possession has been taken of a postal article under subsection (2), the authorised officer who executes the interception direction and the entry warrant or assists with the execution thereof–
a. shall take proper care of the postal article and may, if the postal article concerned is perishable, with due regard to the interests of the persons concerned, dispose of that postal article in such manner as circumstances may require;

b. shall return the postal article, if it has not been disposed of in terms of paragraph (a), or cause it to be returned to the postal provider if, in the opinion of the authorised officer concerned–
   i. no criminal or civil proceedings as contemplated will be instituted in connection with the postal article, or,
   ii. the postal article will not be required at any such criminal or civil proceedings for purposes of evidence or for purposes or order of the court, and
   iii. such postal article may be returned without prejudice to the national security of Saint Lucia, public safety, public health or economic well being of Saint Lucia as the case may be.

15. Entry on premises for execution of entry warrant

If an entry warrant has been issued under the provisions of this Act, an authorised officer who executes or assists with the execution thereof, may at any time during which the entry warrant is in force, without prior notice to the owner or occupier of the premises specified in the entry warrant, enter the said premises and perform any act relating to the purpose for which the entry warrant has been issued.

16. Duty to provide assistance

(1) A person who provides a public postal service or a telecommunications service by means of a public telecommunications network or a private telecommunications network shall take such steps as are necessary to facilitate the execution of an interception direction or an entry warrant, or both.

(2) Where the authorised officer intends to seek the assistance of any person in executing an interception direction or an entry warrant or both, the judge shall, on the request of the Attorney General or the Director of Public Prosecutions, appearing on behalf of the authorised officer, direct appropriate persons to furnish information, facilities, or technical assistance necessary to accomplish the interception.

(3) A person who knowingly fails to comply with his or her duty under subsection (2) commits an offence and is liable on summary conviction to a fine not exceeding $2,000 or to a term of imprisonment not exceeding 6 months or to both.

(4) An action shall not be brought in any court against a person for any act done in good faith under an interception direction or an entry warrant or both, to provide information, facilities or technical assistance under subsection (2).

(5) A person directed to provide assistance by way of information, facilities, or technical assistance pursuant to subsection (2), shall promptly comply in such a manner that the assistance is rendered–
   a. as unobtrusively; and
   b. with the minimum interference to the services that such a person or entity normally provides to the party affected by the interception direction or entry warrant, as can reasonably be expected in the circumstances.

(6) For the purposes of this section, the provision of information facilities or technical assistance includes any disclosure of intercepted material and related communications data to the authorised officer.

St. Vincent and the Grenadines – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Suriname – NONE

Trinidad and Tobago – NONE

5.6 Confidentiality Measures

- The legislative framework provides adequate mechanisms for keeping intercepted communications confidential.
- There are limited exceptions to non-disclosure of intercepted communications provided in the law.

Antigua and Barbuda – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

The Bahamas – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Barbados – NONE

Belize – NONE

Dominica – LIMITED
*Limited, legislative framework proposed based on OECS Model and EUSFA Review. Bill in Parliament as at September 2009.

Dominican Republic – NONE

Grenada – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Guyana – NONE

Haiti – NONE

Jamaica – GOOD

Interception of Communications Act, , No. 5 of 2002 and No. 18 of 2006

St. Kitts and Nevis – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Saint Lucia – GOOD

Interception of Communications Act, Cap. 3.12.

17. Confidentiality of intercepted communications

(1) Where a judge issues an interception direction or an entry warrant, he or she shall issue the interception direction or entry warrant as he or she considers appropriate for the purpose of requiring the authorised officer to make such arrangements as are necessary for ensuring that regulations made under section 36(2)(b) and (c) are complied with.

(2) Where any record is made, whether in writing or otherwise, of any communication obtained by means of an interception direction or an entry warrant or both, the person to whom the interception direction or the entry warrant or both, is issued shall, as soon as possible after the record has been made, cause to be destroyed after a prescribed period, so much of the record as does not relate directly or indirectly to the purposes for which the interception direction or the entry warrant was issued or is not required for the purposes of any prosecution for an offence.

(3) A person who fails to comply with subsection (2) commits an offence and is liable, on summary conviction, to a fine not exceeding $2,000 or to imprisonment for a term not exceeding 6 months.

St. Vincent and the Grenadines – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Suriname – NONE

Trinidad and Tobago – NONE

5.7 Monitoring Measures

- The law does not allow for the fact of interception or the content of intercepted communications to be disclosed in legal proceedings or to be admissible used in evidence.
- The law provides exception to the rule on inadmissibility.

Antigua and Barbuda – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

The Bahamas – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Barbados – NONE

Belize – NONE

Dominica – LIMITED
*Limited, legislative framework proposed based on OECS Model and EUSFA Review. Bill in Parliament as at September 2009.

Dominican Republic – NONE

Grenada – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Guyana – NONE

Haiti – NONE

Jamaica – GOOD

Section V

Interception of Communications Act, No. 5 of 2002 and No. 18 of 2006

The Act came into force on 15th March 2002 and was amended in 2006.

St. Kitts and Nevis – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Saint Lucia – GOOD

Interception of Communications Act, Cap. 3.12.

18. Exclusion of matters from legal proceedings

(1) Subject to section 19, no evidence shall be adduced, question asked, assertion or disclosure made, or other thing done, for the purposes of or in connection with any legal proceedings which, in any manner–

a. discloses, in circumstances from which its origin in anything specified in subsection (2) may be inferred, any of the contents of intercepted communications data; or
b. tends, apart from any such disclosure, to suggest that anything specified in subsection (2) has or may have occurred or is going to occur.

(2) The circumstances referred to in subsection (1) are as follows–

a. conduct by a person falling within subsection (3) that was or would be an offence under section 3(1);
b. the issue of an interception direction or an entry warrant or both;
c. the making of an application by the Attorney General or the Director of Public Prosecutions on behalf of an authorised officer, for an interception direction or an entry warrant or both;
d. the imposition of any requirement on any person to provide assistance with giving effect to an interception direction or an entry warrant.

(3) The persons referred to in subsection (2)(a) are–

a. any person to whom an interception direction or an entry warrant pursuant to this Act may be addressed;
b. any person holding office under the Crown;
c. any person employed by or for the purposes of the Police Force or the Financial Intelligence Authority;
d. any person providing a postal service or employed for the purposes of any business of providing a postal service; and
e. any person providing a telecommunications service or an employee for the purposes of any business of providing such a service.

19. Exceptions to section 18

(1) Section 18 shall not apply to–

a. any application to a judge under this Act;
b. any proceedings for a relevant offence; and
c. proceedings before the Tribunal in relation to an offence committed pursuant to the provisions of this Act.

(2) Section 18 shall not prohibit anything done in, for the purposes of, or in connection with, so much of any legal proceedings as relates to the lawfulness of a dismissal on the grounds of any conduct constituting an offence under section 3(1), or section 22.

(3) Section 18(1)(a) shall not prohibit the disclosure of any contents of a communication if the interception of that communication does not constitute an offence by virtue of section

3(2)(b), (c), (d) or section 3(3).

(4) Where any disclosure is proposed to be or has been made on the grounds that it is authorised by subsection (3), section 18(1) shall not prohibit the doing of anything in or for the purposes of, so much of any legal proceedings as relates to the question whether that disclosure is or was so authorised.

(5) Section 18(1)(b) shall not prohibit the doing of anything that discloses any conduct of a person for which he or she has been convicted of an offence under section 3(1), 16 or 22.

(6) Nothing in section 18(1) shall prohibit any such disclosure of any information that continues to be available as is confined to a disclosure to a person conducting a criminal prosecution for the purpose only of enabling that person to determine what is required of him or her by his or her duty to secure the fairness of the prosecution.

(7) For the purposes of this section "relevant offence" means–

a. an offence under any provision of this Act;
b. an offence under the Telecommunications Act;
c. perjury in the course of any proceedings mentioned in subsection (1) or subsection (2);
d. attempting or conspiring to commit, or aiding, abetting, counselling or procuring the commission of, an offence falling within any of the preceding paragraphs; and
e. contempt of court committed in the course of, or in relation to, any proceedings mentioned in subsection (1) or subsection (3).

20. Offence for unauthorised disclosure of interception

(1) Where an interception direction or an entry warrant or both, has been issued or renewed, it shall be the duty of every person mentioned under section 18(3) to keep such information confidential–

a. the existence and the contents of the interception direction and the entry warrant;
b. the details of the issue of the interception direction and the entry warrant and of any renewal or modification of either;
c. the existence and the contents of any requirement to provide assistance with the giving effect to the interception direction or the entry warrant;
d. the steps taken under the interception direction or the entry warrant or of any such requirement; and
e. everything in the intercepted material together with any related communications data.

(2) A person who makes a disclosure to any person of anything that he or she is required to keep confidential under subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding one year or to both.

(3) In relation to proceedings against any person for an offence under this section in respect of any disclosure, subsections 4(8) to 4(11) shall apply with any necessary modification as they apply in relation to proceedings under section 4.

(4) In proceedings against any person for an offence under this section in respect of any disclosure, it shall be a defence for that person to show that the disclosure was confined to a disclosure authorised–

a. by the interception direction or the entry warrant or by the person to whom the interception direction or the entry warrant is or was addressed; or
b. by section 16.

21. Order requiring disclosure of protected information

Section V

(1) Where protected information has come into the possession of an authorised officer by virtue of an interception direction or an entry warrant or both, under this Act, or by means of the exercise of a statutory power to seize, detain, inspect, search or otherwise to interfere with documents or other property, or is likely to do so, or has otherwise come into possession of an authorised officer by any other lawful means, and he or she has reasonable grounds to believe that–

a. a key to the protected information is in the possession of any person; and
b. disclosure of the information is necessary for any of the purposes specified in section 5(1)(a)(i) or (ii);

the Attorney General or the Director of Public Prosecutions may apply in the prescribed form on his or her behalf to a judge in chambers for a disclosure order requiring the person whom he or she believes to have possession of the key to provide disclosure in respect of the protected information.

(2) A disclosure order under subsection (1)–

a. shall–
   i. be in writing in the prescribed form,
   ii. describe the protected information to which the order relates,
   iii. specify the time by which the order is to be complied with, being a reasonable time in all the circumstances, and
   iv. set out the disclosure that is required by the order, and the form and manner in which the disclosure is to be made; and
b. may, require the person to whom it is addressed to keep confidential the contents of the existence of the order.

(3) A disclosure order under this section shall not require the disclosure of any key which–

a. is intended to be used for the purposes only of generating electronic signatures; and
b. has not in fact been used for any other purpose.

(4) In granting a disclosure order required for the purposes of subsections (1) and (2), the judge shall take into account–

a. the extent and the nature of any protected information to which the key is also a key; and
b. any adverse effect that complying with the order might have on a business carried on by a person to whom the order is addressed;

and shall permit only such disclosure as is proportionate to what is sought to be achieved, allowing, where appropriate, for disclosure in such a manner as would result in the putting of the information in intelligible form other than by disclosure of the key itself.

(5) A disclosure order made under this section shall not require the making of any disclosure to a person other than–

a. the authorised officer named in the disclosure order; or
b. such other person, or description of persons, as may be specified in the disclosure order.

22. Effects of disclosure order

(1) Subject to subsection (2), a person to whom a disclosure order is addressed–

a. shall be entitled to use any key in his or her possession to obtain access to the protected information; and
b. in accordance with the disclosure order, shall disclose the protected information in an intelligible form.

(2) Where a disclosure order requires the person to whom it is addressed to disclose protected

information in an intelligible form, that person shall be taken to have complied with that requirement if–

a. he or she makes instead, a disclosure of any key to the protected information that is in his or her possession; or
b. the disclosure is made in accordance with the order, with respect to the person to whom and the time in which, he or she was required to disclose the information.

(3) When a disclosure order requiring access to protected information or the putting of protected information into intelligible form, is addressed to a person who is–

a. not in possession of the protected information to which the order relates; or
b. incapable, without the use of a key that is not in his or her possession, of obtaining access to the protected information or disclosing it in an intelligible form,

he or she shall be taken to have complied with the order if he or she discloses any key to the protected information that is in his or her possession.

(4) It shall be sufficient for the purposes of complying with a disclosure order for the person to whom it is addressed to disclose only those keys, the disclosure of which is sufficient to enable the person to whom they are disclosed to obtain access to the protected information and to put it in an intelligible form.

(5) Where–

a. the disclosure required by a disclosure order under this section allows the person to whom it is addressed to comply with the disclosure order without disclosing all of the keys in his or her possession; and
b. there are different keys, or combination of keys, in the possession of the person referred to in paragraph (a), the disclosure of which would constitute compliance with the order;

that person may select which of the keys, or combination of keys, to disclose for the purposes of complying with the disclosure order.

(6) Where a disclosure order is addressed to a person who–

a. was in possession of a key to protected information but is no longer in possession of it; and
b. if he or she had continued to have the key to the protected information in his or her possession, would be required by virtue of the order to disclose it; and
c. is in possession of information that would facilitate the obtaining of discovery of the key to the protected information or the putting of the protected information into an intelligible form;

that person shall disclose to the person to whom he or she would have been required to disclose the key, all such information as is mentioned in paragraph (c) for the purpose therein mentioned.

(7) A person who, without reasonable excuse fails to comply with a disclosure order commits an offence and is liable on summary conviction on indictment to a fine not exceeding $5,000 or to a term of imprisonment not exceeding one year or to both.

(8) A person who obtains a disclosure order shall ensure that such arrangements are made as are necessary for ensuring that–

a. a key disclosed under the disclosure order is used to obtain access to or put into intelligible form only the protected information in relation to which the order was given;
b. every key disclosed under the disclosure order is stored, for so long as it is retained, in a secure manner, and any records of such key are destroyed as soon as no longer needed to access the information or put it in an intelligible form; and
c. the number of–
   i. persons to whom the key is disclosed or otherwise made available, and

ii. copies made of the key,

is limited to the minimum that is necessary for the purpose of enabling the protected information to be accessed or put into an intelligible form.

(9) Subject to subsection (10) of this section, where any relevant person incurs any loss or damage as a consequence of a breach by a person referred to in subsection (8) of the duty imposed upon him or her by that subsection, the breach shall be actionable against the person referred to in subsection (8) at the suit or instance of the relevant person.

(10) A person is a relevant person for the purposes of subsection (9) if he or she is–

a. a person who has made a disclosure in pursuance of a disclosure order made under section 21; or
b. a person whose protected information or key has been disclosed under a disclosure order made under section 21,

and loss or damage shall be taken into account for the purposes of section 21 to the extent only that it relates to the disclosure of a particular protected information or a particular key which, in the case of a person falling within paragraph (b), shall be his or her information or key.

(11) For the purposes of subsection (10)–

a. information belongs to a person if he or she has any right that would be infringed by an unauthorised disclosure of the information; and
b. a key belongs to a person if it is a key to information that belongs to him or her or he or she has any right that would be infringed by an unauthorised disclosure of the key.

23. Tipping off

(1) This section applies where a disclosure order under section 21 contains a provision requiring–

a. the person to whom the disclosure order is addressed; and
b. every other person who becomes aware of it or of its contents,

to keep confidential the making of the disclosure order, its contents and the things done pursuant to it.

(2) A disclosure order made under section 21 shall not contain a requirement to keep anything secret except where the protected information to which it relates has come, or is likely to come, into possession of an authorised officer by means which it is reasonable, in order to maintain the effectiveness of any investigation or operation or of investigatory techniques generally, or in the interests of safety or well-being of any person, to keep confidential from a particular person.

(3) Any person who makes a disclosure to any other person of anything that he or she is required by a disclosure order under section 21 to keep confidential, commits an offence and is liable, on summary conviction, to a fine not exceeding $5,000 or to a term of imprisonment not exceeding one year.

(4) In proceedings against any person for an offence under this section in respect of any disclosure, it shall be a defence for that person to show that–

a. the disclosure was effected entirely by the operation of software designed to indicate when a key to protected information has ceased to be secure; and
b. the person could not reasonably have been expected to take steps, after the disclosure order was issued to him or her or, as the case may be, on becoming aware of it or of its contents, to prevent the disclosure.

(5) Subsections 4(8) to 4(10) shall apply, with necessary modifications, in relation to proceedings for

an offence under this section as they apply in relation to proceedings for an offence under that section.

(6) In proceedings against any person for an offence under this section, it shall be a defence for that person to show that the disclosure was confirmed to a disclosure authorised–

a. by the terms of a disclosure order made under section 21; or
b. by or on behalf of a person who–
   i. is in lawful possession of the protected information to which it relates, and
   ii. came into the possession of that protected information as mentioned in section 21(1).

(7) In proceedings for an offence under this section against a person other than the person to whom the disclosure order under section 21 was addressed, it shall be a defence for the person against whom the proceedings are brought to show that he or she neither knew nor had reasonable grounds for suspecting that the order contained a requirement to keep confidential what was disclosed.

PART 5

COMMUNICATIONS DATA

24. Disclosure of communications data

(1) For the purposes of this section–

"**designated person**" means the Minister or person designated for the purposes of this section by the Minister by order published in the *Gazette*;

"**traffic data**" in relation to a communication, means any communication data–

a. identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted, and "data" in relation to a postal article, means anything written on the outside of the postal article;
b. identifying or selecting, or purporting to identify or select, apparatus through or by means of which the communication is or may be transmitted;
c. comprising signals for the actuation of–
   i. apparatus used for the purposes of a telecommunications network for effecting, in ii.whole or in part, the transmission of any communications, or
   any telecommunications network in which that apparatus is comprised;
d. identifying the data or other data as data comprised in or attached to a particular communication; or
e. identifying a computer file or a computer programme, access to which is obtained or which is run by means of the communication, to the extent only that the file or the programme is identified by reference to the apparatus in which it is stored, and references to traffic data being attached to a communication include references to the data and the communication being logically associated with each other.

(2) Where it appears to the designated person that a telecommunications provider is or may be in possession of, or capable of obtaining, any communications data, the designated person may, by notice in writing, require the telecommunications provider–

a. to disclose to an authorised officer all of the data in his or her possession or subsequently obtained by him or her, or
b. if the telecommunications provider is not already in possession of the data, to obtain the data and to disclose the data to an authorised officer.

(3) A designated person shall not issue a notice under subsection (2) in relation to any communications data unless he or she is satisfied that it is necessary to obtain the data and

to disclose the data to an authorised officer so disclose it.

(4) A designated person shall not issue a notice under subsection (2) in relation to any communication data unless he or she is satisfied that it is necessary to obtain that data–

a. in the interests of national security;
b. for the purpose of preventing or detecting an offence specified in the Schedule where there are reasonable grounds to believe that such an offence is being or may be committed;
c. in the interests of public order;
d. in the interests of public morality;
e. in the interest of public health;
f. for the purpose in an emergency, of preventing death, injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or

(4) A notice under this section shall state–

a. the communication data in relation to which it applies;
b. the authorised officer to whom the disclosure is to be made;
c. the manner in which the disclosure is to be made;
d. the matters falling within subsection (3) by reference to which the reference is issued; and
e. the date on which it is issued.

(5) A notice under this section shall not require–

a. any communications data to be obtained after the end of the period of one month beginning on the date on which the notice is issued; or
b. the disclosure, after the end of such period, of any communications data not in the possession of the provider of the telecommunications service, or required to be obtained by him or her, during that period.

(6) The provisions of sections 21 and 22 shall apply, with necessary modifications, in relation to the disclosure of data under a notice under to this section.

(7) Subject to subsection (8), a provider of a telecommunications service, to whom a notice is issued under this section, shall not disclose to any person the existence or operation of the notice, or any information from which such existence or operation could reasonably be inferred.

(8) The disclosure referred to in subsection (7) may be made to–

a. an officer or agent of the service provider for the purpose of ensuring that the notice is complied with; or
b. an attorney-at-law for the purpose of obtaining legal advice or representation in relation to the notice;

and a person referred to in paragraph (a) or (b) shall not disclose the existence or operation of the notice, except to the authorised officer specified in the notice for the purpose of–

i. ensuring that the notice is complied with, or obtaining legal advice or representation in relation to the notice, in the case of an officer or agent of the service provider; or
ii. giving legal advice or making representations in relation to the notice, in the case of an attorney-at-law.

(9) A person shall not disclose any communications data obtained under this Act, except–

a. as permitted by the notice;
b. in connection with the performance of his or her duties; or
c. where if the Minister directs that the disclosure be made to a foreign Government or agency of a foreign Government where there exists between Saint Lucia and that foreign Government an agreement for the mutual exchange of that kind of information and the Minister considers it to be in the public interest that such disclosure be made.

(10) A person who contravenes subsection (7), (8) or (9) commits an offence and is liable, on summary conviction, to a fine not exceeding $5,000 or to a term of imprisonment for a term not exceeding one year or to both.

25. Admissibility of communications data

(1) Subject to section 18 and section 19, and to subsection (2) of this section, communications data submitted as evidence in any proceedings under this Act shall be admissible in evidence in accordance with the law relating to the admissibility of evidence.

(2) In admitting into evidence any communications data referred to in subsection (1)–

a. no question shall be asked of any witness that discloses or might result in the disclosure of any of the details pertaining to the method by which the data was obtained of the identity of any party who supplied the data;
b. statement by the witness that the data was obtained by virtue of a disclosure order under section 21 shall be sufficient disclosure as to the source or origin of the data; and
c. in proving the truth of a statement referred to in paragraph (b), the witness shall not be asked to disclose any of the matters referred to in paragraph (a).

(3) Subsection (2) shall not apply to any proceeding in respect of an offence under this Act but if the court is satisfied that–

a. the disclosure is would be likely to jeopardise the course of any investigations or be prejudicial to the interests of national security; and
b. the parties to the proceedings would not be unduly prejudiced thereby, the court shall not require or permit disclosure of the matters referred to in subsection (2)(a).

St. Vincent and the Grenadines – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Suriname – NONE

Trinidad and Tobago – NONE

5.8 Interception Capabilities

- The legislative framework provides for approval or authorization of equipment with interception capabilities.
- Adequate provision is made in the legislation for protection of the technology.

Antigua and Barbuda – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

The Bahamas – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Barbados – NONE

Belize – NONE

Dominica – LIMITED

*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Dominican Republic – NONE

Grenada – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Guyana – NONE

Haiti – NONE

Jamaica – GOOD

Interception of Communications Act, No. 5 of 2002 and No. 18 of 2006

St. Kitts and Nevis – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Saint Lucia – GOOD

Interception of Communications Act, Cap. 3.12.

26. Listed equipment

(1) Subject to subsection (4) the Minister may, by order published in the Gazette, declare any electronic, electro magnetic, acoustic, mechanical or other instrument, device or equipment, the design of which renders it primarily useful for purposes of the interception of communications, under the conditions or circumstances specified in the order.

(2) An order under subsection (1) may at any time in like manner be amended or withdrawn.

(3) The first order to be issued by the Minister under subsection (1) shall be published in the Gazette within 3 months after the date of commencement of this Act.

(4) Subject to subsection (6), before the Minister exercises the powers conferred upon him or her under subsection (1), he or she shall cause to be published in the Gazette a draft of the proposed order, together with a notice inviting all interested parties to submit to him or her in writing and within a specified period, comments and representations in connection with the proposed order.

(5) A period not exceeding one month shall elapse between the publication of the draft order and the publication of the order under subsection (1).

(6) Subsection (4) of this section shall not apply–

a. if the Minister, under comments and representations received in terms of subsection (4) decides to publish an order referred to in subsection (1) in an amended form; or
b. to any declaration in terms of subsection (1) in respect of which the Minister is of the opinion that the public interest requires that it be made without delay.

(7) An order under subsection (1) shall be subject to affirmative resolution of the House of Assembly and Senate.

27. Prohibition on manufacture and possession of listed equipment

(1) Subject to subsection (2) and section 28, a person shall not manufacture, assemble, possess, sell, or purchase any listed equipment.

(2) Subsection (1) shall not apply to any authorised officer or any other person who manufactures, assembles, possesses, sells, purchases, or advertises listed equipment under the authority of a certificate of exemption issued to him or her by the Minister under section 28.

28. Exemptions

(1) The Minister may, upon application made by a person in the prescribed form, and acting upon the advice of Cabinet, exempt a person from one or all of the prohibited acts listed under section 27(1) for such period and on such terms as the Minister may determine.

(2) The Minister shall not grant an exemption under subsection (1) unless he or she is satisfied that–

a. the exemption is in the public interest; or
b. special circumstances exist which justify the exemption.

(3) An exemption under subsection (1) of this section shall be granted by issuing to the person concerned, a certificate of exemption, in the prescribed form in which his or her name, and the scope, period and conditions of the exemption are specified.

(4) A certificate of exemption granted pursuant to subsection (3) shall be published in the Gazette and shall become valid upon the date of such publication.

(5) A certificate of exemption may at any time in like manner be amended or withdrawn by the Minister.

(6) A certificate of exemption lapses upon–

a. termination of the period for which it was granted; or
b. withdrawal under subsection (5).

29. Offence for contravention of section 27

(1) A person who contravenes or fails to comply with section 27 commits an offence and is liable on summary conviction to a fine not exceeding $25,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) A court convicting a person of an offence under subsection (1) of this section shall in addition to any penalty which it may impose in respect of the offence, declare any listed equipment–

a. by means of which the offence was committed;
b. which was used in connection with the commission of the offence;
c. which was found in the possession of the convicted person; or
d. the possession of which constituted the offence, to be forfeited to the Crown.

(3) Where a person is convicted of an offence referred to in subsection (1), the court shall, in addition to the penalty which it may impose in respect of the offence, declare forfeited to the State any equipment other than listed equipment which was found in the possession of the convicted person and–

a. the possession of which constitutes an offence;
b. by means of which the offence was committed; or
c. which was used in connection with the commission of the offence.

(4) Any listed equipment or other equipment declared forfeited under subsection (2) or (3) of this section shall, as soon as practicable after the date of declaration of forfeiture be delivered to the Commissioner of Police.

(5) Any listed equipment or other equipment delivered to the Commissioner of Police under subsection (4) shall, in the case of–

Section V

a. listed equipment declared forfeited under subsection (2) of this section, be kept by the Commissioner of Police;
   i. for a period not exceeding 4 months with effect from the date of declaration of forfeiture; or
   ii. if an application under subsection (8) is made, pending the final decision in respect of any such application has been given; or
b. equipment declared forfeited under subsection (3) of this section, be kept by the Commissioner of Police for a period not exceeding 30 days with effect from the date of declaration of forfeiture and shall as soon as practicable after the expiry of the period of 30 days referred to be destroyed by the Commissioner of Police.

(6) The Commissioner shall–
a. as soon as practicable after the expiry of the period referred to in subsection (5)(a)(i);
b. if the decision referred to in subsection (5)(a)(ii) has been given against the person making the application; or
c. if an application referred to in subsection (5)(a)(ii) has been refused,

destroy such listed equipment or other equipment in his or her possession.

(7) A declaration of forfeiture under subsection (3) shall not affect any right which a person, other than the convicted person, may have to the listed equipment, if the person can show that–
a. he or she has been exempted under section 28 from the relevant prohibited act referred to in section 27 in respect of such listed equipment;
b. he or she has taken all reasonable steps to prevent the use thereof in connection with the offence; and
c. could not reasonably be expected to have known or had no reason to suspect that the listed equipment concerned was being or would be used in connection with the offence.

(8) The judge may, upon an application made at any time within a period of 3 months with effect from the date of declaration of forfeiture under subsection (3), by any person other than the convicted person, who claims that–
a. the listed equipment declared forfeited under subsection (3) is his or her property; and
b. he or she is a person referred to in subsection (9),

inquire into and determine those matters.

(9) If the judge under subsection (8) is satisfied that the–
a. listed equipment concerned is the property of the person; and
b. the person concerned is a person referred to in subsection (8),

the judge shall set aside the declaration of forfeiture and direct that the listed equipment concerned be returned to the person.

St. Vincent and the Grenadines – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Suriname – NONE

Trinidad and Tobago – NONE

5.9 Internal Safeguard Measures

- Internal safeguard measures are provided for in the law.
- The law provides for monitoring by an independent authority.

Antigua and Barbuda – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

The Bahamas – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Barbados – NONE

Belize – NONE

Dominica – LIMITED
*Limited, legislative framework proposed based on OECS Model and EUSFA Review. Bill in Parliament as at September 2009.

Dominican Republic – NONE

Grenada – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Guyana – NONE

Haiti – NONE

Jamaica – GOOD

Interception of Communications Act, No. 5 of 2002 and No. 18 of 2006

The Act came into force on 15th March 2002 and was amended in 2006.

St. Kitts and Nevis – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Saint Lucia – GOOD

Interception of Communications Act, Cap. 3.12.

Reports on progress

A judge who has issued an interception direction or an entry warrant or both, may at the time of issuance or at any stage before the date of expiry thereof, in writing require the authorised officer, on whose behalf the relevant application was made in respect of the interception direction or the entry warrant or both, to report to him or her in writing–

a. at such intervals as he or she determines on–
   i. the progress that has been made towards achieving the objectives of the interception direction or the entry warrant or both; and
   ii. any other matter which the judge deems necessary; or
b. on the date of expiry of the entry warrant and interception direction concerned, on whether the interception device has been removed from the premises and, if so, the date of such removal.

St. Vincent and the Grenadines – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Suriname – NONE

Trinidad and Tobago – NONE

5.10 Dispute Resolution

- The law makes adequate provision for dispute resolution.
- There is an appropriate body established or designated with adequate powers to deal with dispute resolution.
- Adequate remedies are provided by the legislative framework.

Antigua and Barbuda – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

The Bahamas – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Barbados – NONE

Belize – NONE

Dominica – LIMITED
*Limited, legislative framework proposed based on OECS Model and EUSFA Review. Bill in Parliament as at September 2009.

Dominican Republic – NONE

Grenada – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Guyana – NONE

Haiti – NONE

Jamaica – GOOD

Interception of Communications Act, 5 of 2002 as amended by of 2006

St. Kitts and Nevis – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Saint Lucia – GOOD

Interception of Communications Act, Cap. 3.12.

30. Establishment of Tribunal

(1) There shall be established, for the purpose of exercising jurisdiction conferred upon it by this section, a Tribunal consisting of a judge who shall be appointed by the Chief Justice acting on his or her own deliberate judgement.

(2) The jurisdiction of the Tribunal shall–

a. be the only forum for the purposes of any proceedings under any law of Saint Lucia which shall fall within subsection (3);
b. to consider and determine any complaints made to the Tribunal which, in accordance with subsection (4), are complaints for which the Tribunal is the appropriate forum; and
c. to consider and determine any reference to the Tribunal by any person that he or she has suffered detriment as a consequence of any prohibition or restriction, by virtue of section 21, on his or her relying in, or for the purposes of, any civil proceedings on any matter.

(3) The following proceedings shall be subject to this section–

a. proceedings brought by virtue of section 22(9); or
b. proceedings relating to the taking place in any challengeable circumstances of any conduct falling within subsection (5).

(4) The Tribunal shall be the appropriate forum for any complaint if it is a complaint by a person who is aggrieved by any conduct falling within subsection (5), which he or she believes–

a. to have taken place in relation to him or her, to any communications sent by him or her, or intended for him or her, or to his or her use of any postal service, telecommunications service or telecommunications network; and
b. to have taken place in challengeable circumstances.

(5) The following conduct shall be subject to this section–

a. conduct for or in connection with the interception of communications in the course of its transmission by means of a postal service or a telecommunications service; or
b. any disclosure or use of a key to protected information.

(6) For the purposes of this section conduct takes place in challengeable circumstances if–

a. it is conduct by or on behalf of a person holding any office, rank or position in the Police Force or the Financial Intelligence Authority, or any other position within the Government service, and
b. the conduct took place without the authority of an interception direction or an entry warrant, or otherwise without authority under this Act.

(7) Without prejudice to subsection (6), conduct does not take place in challengeable circumstances to the extent that it is authorised by, or takes place with the permission of, a judicial authority.

(8) For the purposes of subsection (7) "judicial authority" means a judge or a magistrate.

31. Exercise of the Tribunal's jurisdiction

(1) The Tribunal shall not be under any duty to hear, consider or determine any proceedings, complaint or reference if it appears to it that the bringing of the proceedings or the making of the complaint or reference is frivolous or vexatious.

(2) Except where the Tribunal, having regard to all the circumstances, is satisfied that it is equitable to do so, it shall not consider any complaint made by virtue of section 30(2)(b) if it is made more than one year after the taking place of the conduct to which it relates.

(3) Subject to any provision made by the rules under section 33, where any proceedings have been brought before the Tribunal or any reference made to the Tribunal, it shall have power to make such interim orders, pending its final determination, as it thinks fit.

(4) Subject to any provision made by rules under section 33, the Tribunal on determining any proceedings, complaint or reference shall have the power to make any award of compensation or other order as it thinks fit, including an order requiring the destruction of

any records of information, which is held by any public authority in relation to any person.

(5) Appeals from determinations, awards, orders and other decisions of the Tribunal, shall lie to the Court of Appeal.

32. Tribunal procedure

(1) Subject to any rules made under section 33, the Tribunal shall be entitled to determine its own procedure in relation to any proceedings, complaint or reference brought before or made to it.

(2) In determining its procedure under this section, the Tribunal shall have regard in particular to–

a. the need to ensure that matters which are the subject of proceedings, complaints or references brought before or made to the Tribunal are properly heard and considered; and
b. the need to ensure that information is not disclosed to an extent, or in a manner, that is contrary to the public interest or prejudicial to national security or the prevention or detection of serious crime, and without prejudice to the generality of the foregoing, may in particular follow any procedure mentioned in section 33(4) for that purpose.

(3) Where the Tribunal determines any proceedings, complaint or reference brought before or made to it, it shall give–

a. a statement that the Tribunal has made a determination in favour of the person making the complaint; or
b. a statement that no determination has been made in favour of the person making the complaint.

33. Tribunal rules

(1) The Chief Justice may make rules regulating–

a. he exercise by the Tribunal of the jurisdiction conferred on it by section 30(2); and
b. any matters preliminary or incidental to, or arising out of, the hearing or consideration of any proceedings, complaint or reference brought before or made to the Tribunal.

(2) Without prejudice to the generality of subsection (1), rules under this section may–

a. specify the forms of hearing or consideration to be adopted by the Tribunal in relation to particular proceedings, complaints or references, including where applicable, the mode and burden of proof and the admissibility of evidence;
b. require information about any determination, award, order or other decision made by the Tribunal in relation to any proceedings, complaint or reference to be provided, in addition to any statement under section 32(3) to the person who brought the proceedings or made the complaint or reference to the person representing his or her interests.

(3) Rules made under this section may provide–

a. for a person who has brought any proceedings before or made any complaint or reference to the Tribunal to have the right to be legally represented;
b. for the manner in which the interests of a person who has brought any proceedings before or made any complaint or reference to the Tribunal are otherwise to be represented;
c. for the appointment in accordance with the rules, by such person as may be determined by the rules, of a person to represent those interests in the case of any proceedings, complaint or reference.

(4) Rules made under this section may in particular enable or require the Tribunal to proceed in the absence of any person, including the person making the complaint or reference and any

legal representative of the person, and to exercise its jurisdiction, and to exercise and perform its powers and duties, including in particular, in relation to the giving of reasons, in such a manner provided for in the rules as prevents or limits the disclosure of particular matters.

(5) Rules made under this section may make application, with or without modification, of the provision from time to time contained in specified rules of court.

(6) All rules made under this section shall be subject to affirmative resolution of the House of Assembl

St. Vincent and the Grenadines – LIMITED
*Limited, legislative framework proposed in the OECS Interception of Communications Bill.

Suriname – NONE

Trinidad and Tobago – NONE

Section VI:
Comparative Law Analysis

The inventory of legislation on interception of communication in the Beneficiary Member States, as pictured in Section 5 above (and in Section 7 below), has evidenced that the current panorama falls into three basic categories: i) States with good, existing legislation (Jamaica and Saint Lucia); ii) States with proposed good legislation (inspired by the OECS Interception of Communications Bill); and iii) States with no existing or proposed legislation.

Therefore, comparative law analysis, herein circumscribed to a selection among existing differences, must focus on the national laws of Jamaica and of Saint Lucia, as well as on the OECS Interception of Communications Bill, to compare with the sample legislation quoted in Section 4 above.

The comparative analysis to follow initially stresses different formal approaches, and then go over diverse treatment given to substantive matters.

6.1 Jamaica

Jamaica's Interception of Communications Act, in its Section 2, defines **"intercept"** as comprising the:

a. "monitoring of transmissions made by wireless telegraphy to or from apparatus comprising in the network;

b. monitoring or modification of, or interference with, the network by means of which the communication is transmitted, so as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication, and "interception" shall be construed accordingly;"

Differently, ITU's Toolkit for Cybercrime Legislation, in its Section 1, (k), defines "interception" as follows:

"Interception" means the acquisition, viewing, capture, or copying of the contents or a portion thereof, of any communication, including content data, computer data, traffic data, and/or electronic emissions thereof, whether by wire, wireless, electronic, optical, magnetic, oral, or other means, during transmission through the use of any electronic, mechanical, optical, wave, electromechanical, or other device."

ITU's proposed wording seems clearer to the effect of including the acquisition, capture and copying of intercepted communication. While one might argue that these actions are included in the generic language "to make (…) available", present in the Jamaican text, specific language is especially important in the criminal field, where no ambiguity or analogy are allowed to unfavor the suspected party.

Also, the list of subjects ("content data, computer data, traffic data, and/or electronic emissions thereof") and of media ("wire, wireless, electronic, optical, magnetic, oral, or other means, during transmission through the use of any electronic, mechanical, optical, wave, electromechanical, or other device") subject to interception of communication is present in the very definition of interception. From a systemic point of view, this may make easier to enforce such kind of provision than in the option adopted in the Jamaican law, which relies on an extensive roll of other definitions in Section 2[45] and on another roll of definitions in Section 16[46], to complete the meaning of "intercept".

---

[45] Some definitions use terminology not consistent with the ones often found in international legislation; for instance, the definition of "telecommunications" as "transmission of intelligence", while in Section 16, "b", "communication data" are defined as comprising "information".

[46] The placement of important definitions such as of "communications data" and of "traffic data" at the ending portion of the Law (Section 16), as opposed to most definitions, which are included in the beginning of the Law (Section 2), seems not compatible with the systemic approach followed in international laws.

Regarding illegal interception, Jamaica's Interception of Communications Act establishes the following:

"3.-(1) Except as provided in this section, a person who intentionally intercepts a communication in the course of its transmission by means of a telecommunications network commits an offence and is liable upon summary conviction in a Resident Magistrate's Court to imprisonment for a term not exceeding three years or to a fine not exceeding three million dollars or to both such fine and imprisonment."

In comparison, the Budapest Convention on Cybercrime regulates such misconduct as follows:

"Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system."

At first sight, comparing only the first paragraph of the paradigm text and of Jamaica's, the former seems more complete, as it is more specific on the media subject to interception of communication, in the same paragraph. However, Jamaica's list of hypothesis which exempt from falling under the head of its provision is very comprehensive and coherent.

Regarding warrants for interception, Jamaica's Interception of Communications Act sets forth the following:

4.-(1) Subject to the provisions of this section, an authorized officer may apply ex parte to a Judge in Chambers for a warrant authorizing the person named in the warrant-

a. to intercept, in the course of their transmission by means of a public or private telecommunications network, such communications as are described in the warrant; and
b. to disclose the intercepted communication to such persons and in such manner as may be specified in the warrant.

(2) A Judge shall not issue a warrant under this section unless he is satisfied that-

a. the warrant is necessary-
    i. in the interests of national security; or
    ii. for the prevention or detection of any offence specified in the Schedule, where there are reasonable grounds for believing that such na offence has been, is being or is about to be committed;
b. information obtained from the interception is likely to assist in investigations concerning any matter mentioned in paragraph (a);
c. other investigative procedure:
    i. have not been or are unlikely to be successful in –attaining the information sought to be acquired by means of the warrant;
    ii. are too dangerous to adopt in the circumstances; or
    iii. having regard to the urgency of the case are impracticable; and it would be in the best interest of the administration of justice to issue the warrant.

On the matter, Australian TIA provides for two types of interception warrants:

- a "telecommunications service" warrant[47] which authorises the interception of only one service at a time, for example, one telephone number.
- a "named person" warrant (s46A) authorises the interception of more than one telecommunications service used or likely to be used by the person the subject of the warrant (i.e. it may authorise interception of one or more telephone services and/or also interception of one or more email services, etc).[48]

Jamaica's provision on the grant of interception warrants seems quite complete, about the goals and the requirements of a warrant. The Australian text is practical, with regard to the scope and finality of the two modalities of warrant.

In general terms, the Jamaican law is, from the substantive standpoint, fairly in line with the comprehensiveness and treatment observed in international trends and best practices.

Possible further improvements in the scope49 and terminology of definitions, as well as in the systemic placement of some provisions might reinforce compatibility of Jamaica's Law with the patterns found in international laws.

6.2 Saint Lucia

The law enacted by Saint Lucia – Telecommunications (Confidentiality in Network and Services) Regulations, nr. 17, of 2002 – is a concise piece of legislation, which may be complemented in the event Saint Lucia's Privacy and Data Protection Bill comes into law, as the latter contains a part focusing on exemption from data protection, as follows:

PART 6

EXEMPTIONS

National Security

51. The Minister may by Order published in the Gazette exempt a data controller from complying with any provision of this Act in the interest of national security.

Crime and taxation

52. A data controller which is a public authority shall be exempt from the provisions of Parts 3, 4 and 5 if the processing of data is required for-

a. the prevention or detection of crime;
b. the apprehension or prosecution of offenders; or
c. the assessment or collection of any tax, duty or any imposition of a similar nature,

6.3 OECS

In OECS' Interception of Communications Bill, "intercept" is defined as:

"intercept" means the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes the;

---

47 Section 46.

48 Electronic Frontiers Australia, Telecommunications Interception & Access Laws, 2006,at pages 6.

49 For instance, in the definition of "traffic data", Jamaica's Law misses specification of media which is found in the ITU's Toolkit.

a. monitoring of any such communication by means of a monitoring device;
b. viewing, examining, or inspection of the contents of any communication; and
c. diversion of any communication from its intended destination to any other destination;

and **"interception"** shall be construed accordingly;

In contrast, ITU's Toolkit provides the following definition:
k. Interception

"Interception" means the acquisition, viewing, capture, or copying of the contents or a portion thereof, of any communication, including content data, computer data, traffic data, and/or electronic emissions thereof, whether by wire, wireless, electronic, optical, magnetic, oral, or other means, during transmission through the use of any electronic, mechanical, optical, wave, electromechanical, or other device.

The differences in concept between those definitions echo the ones commented above with regard to Jamaica's law.

With regard to illegal interception, OECS' Bill provide as follows:

Prohibition of interception

3. (1) Except as provided in this section, a person who intentionally intercepts a communication in the course of its transmission by means of a public postal service or a telecommunications network commits an offence and is liable to conviction on indictment to a fine not exceeding seventy thousand dollars or a term of imprisonment not exceeding three years or to both such fine and imprisonment.

The Budapest Convention regulates illegal interception in the following manner:

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

The differences reside, basically, in the more specific terms found in ITU's Toolkit regarding indication of media subject to interception of communication, as well as in the more systemic approach adopted in the latter.

Moving to comparative analysis on substantive matters, the differences perceived are also worth noticing.

6.4 Competent Authorities

Most countries have the Judiciary as the competent Branch in charge of authorizing interception of communication.

Australia

In some other countries, the Attorney General's Office is responsible for issuing interception warrants or directions. This is the case in Australia, where a national security warrant issued by the Attorney General who is the Minister responsible for Legal Affairs and the Australian Security Intelligence Organisation (ASIO) and the police. However in limited circumstances national security warrants which are to expire after 48 hours may be issued by the ASIO's Director General of security who reports to the Attorney General. It is noted that the Attorney General is appointed by the Prime Minister who, by convention, is the leader of the party or coalition which has the most seats in the House of Representatives.

In Australia Law enforcement warrants for interception are issued by a judge of a court created by the Australian Parliament who has consented to be nominated by the Attorney General and who has been declared by the Attorney General to be an eligible Judge.[50] or the Deputy President, a full time or part time senior member or member of the Administrative Appeals Tribunal (AAT) nominated by the Attorney General to issue interception directions.[51]

United Kingdom

In the United Kingdom, the person who issues both certified and normal warrants is a Secretary of State, normally the Home Secretary responsible for law and order in the United Kingdom, who is appointed by the Prime Minister. Even in an urgent case where a warrant can be signed by a senior official, the Secretary of State must have considered the application and given instructions to the official before the signing of that particular warrant.[52]

USA, Jamaica and Saint Lucia

In the USA, as is the case in Saint Lucia and in Jamaica and for some law enforcement warrants in Australia, an interception warrant or direction is issued by a judge. This approach takes advantage of the competence and independence of the Judiciary to assess evidence and make decisions without being tainted by political or partisan influences.

6.5 Definition of Intercept

Definition of the term **"intercept"** (or, "interception"), in any legislative framework, is necessary to set the parameters within the law to apply. Specifically in the context of the legislative framework on interception of communications, the term "interception" must be defined within the context of the policy to be implemented. Generally, "interception" should not be confined to any particular communication handling system and should be broad enough to cover communications sent through various types of networks including telephone networks, e-mail systems or other wireless transmissions.

Australia

The TIA Act 1974 of Australia, in its definition of "intercept", only provides for communications via telecommunications systems by specifying that interception consists of listening to or recording, by any means, such as a communication in its passage over that telecommunications system without the knowledge of the person making the communication53. It is therefore wide enough to encompass communications transmitted via the internet and VOIP.

United Kingdom.

In the United Kingdom, the RIPA presents a construction of the meaning of the term "intercept" which is broad enough to cover wireless transmissions as well as transmissions via telecommunications by providing that a person "intercepts" a communication in the course of its transmission by means of a telecommunication system if, and only if, he so modifies or interferes with the system, or its operation, so monitors transmissions made by means of the system, or so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system as to make some or all of the contents of the communication available, while being transmitted to a person other than the sender or intended recipient of the communication.

---

50 Section 6D, TIA Act 1979.
51 Section 6DA, TIA Act 1979.
52 Thomas Wang, Regulation of interception in selected jurisdictions, 2005, Legislative Council Secretariat.
53 Section 6 Telecommunications (Interception) Act.

United States

Under Title 18 Part 1, Chapter 119, section 2510 of the US Code, interception is defined in technology neutral terms as the aural or other acquisition of the contents of any electronic or oral communications through the use of any electronic mechanism or other device.

Jamaica

The Jamaican Interception of Communications Act defines intercept in relation to a communication as the monitoring of transmissions made by wireless telegraphy to or from apparatus comprising in the network; or monitoring or modification of, or interference with, the network by means of which the communication is transmitted, so as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication.[54]

Saint Lucia

Saint Lucia's Interception of Communications Act defines intercepted communications in technology neutral terms typical of a postal service or of a telecommunications network service, that is, a service using any wire, radio, optical or other electromagnetic system used to route switch or transmit telecommunications)[55].

6.6 Right to Intercept

In order to balance the right to intercept against an individual's fundamental right to privacy, most countries have found it necessary to provide a legislative framework within which interception of communication may be authorised and controlled in a manner commanding public confidence. The intention is usually to control the interception of communication by unauthorized persons by prohibiting interception except within certain narrow circumstances to be determined by an authorized person. This is achieved by criminalizing the acts of persons found intercepting communications except where the interception is authorised on application by specified persons on specific grounds which usually mainly include national security and the detection of crime.

The legislative framework usually specifies the persons who have authority to make applications for lawful interception of communications and the procedure for applications and grant of a warrant for interception. Certain officers are empowered to make applications for warrants for interceptions of communications. These officers may include persons who occupy critical offices in terms of economic and political security of the State.

Australia

The TIA Act of Australia prohibits a person from intercepting, authorising, suffering or permitting another person to intercept or do any act or thing that will enable him or her or another person to intercept a communication passing over a telecommunications system.[56] The penalty for contravention of the prohibition is imprisonment for a period not exceeding 2 years[57] (s105). The limited exceptions to the prohibition are specified to include –

- interception under an interception warrant on grounds of national security or law enforcement;

[54] Section 2, Interception of Communications Act, Jamaica.
[55] Section 2, Interception of Communications Act, Saint Lucia.
[56] Section 7, TIA 1979
[57] Section 105, TIA 1979

- exceptions to enable police to intercept communications in specified urgent situations, and carrier employees on emergency request of police to intercept a communication for the purposes of tracing the location of the caller, where there is risk loss of life or the infliction of serious personal injury or threats to kill or seriously injure another person or to cause serious damage to property, etc;
- exceptions to enable an officer of the Australia Security Intelligence Organisation (ASIO) in the lawful performance of his or her duties, to discover whether a listening device is being used at, or in relation to, a particular place; or determine the location of a listening device; and
- exceptions applicable to carriers and carrier employees in relation to duties involving the installation of lines and equipment or the operation or maintenance of a telecommunications system.

An application for a national security warrant in Australia must be made in writing by the Director General of Security while those for law enforcement warrants may be made by the Australian Federal Police, the Australian Crime Commission or an eligible authority of a State or Northern Territory in which a Ministerial declaration is in force.

United Kingdom

In the United Kingdom, an offence of unlawful interception is created together with a separate civil liability for unlawful interception, which explains the locations and circumstances in which each is applicable and the circumstances in which interception is lawful.

The RIPA establishes a regulatory system under which there are two types of warrant required for lawful interception of communication[58]. The first type usually applied for by intercepting agencies is the "normal warrant", which requires the subject of the interception warrant to be a person or the premises where the interception is to take place. The second type of warrant is known as the "certified warrant" and is exempt from the requirement to specify a subject, but requires a certificate by the Secretary of State and is only applied to external communications sent or received outside of the United Kingdom.

The application for an interception warrant under the RIPA may be made only by or on behalf of a limited number of high level officials[59], including:

- the heads of security and intelligence agencies, namely the Director-General of the Security Service (MI5); the Chief of the Secret Intelligence Service (MI6); the Director of Government Communications Headquarters (GCHQ); the Director-General of the National Criminal Intelligence Service (NCIS); and the Chief of; and Defence Intelligence Staff (DIS)[60].
- the heads of law enforcement agencies, namely the Commissioner of Police of the Metropolis of Northern Ireland; the Chief Constable of any police force maintained under the Police (Scotland) Act 1967; and the Commissioners of Customs and Excise.[61]

Under the RIPA, an interception warrant will only be issued if the Home Secretary believes that it is necessary in the interest of national security[62], for preventing serious crime[63] or for safeguarding the economic well-being of the UK against overseas threats or for giving effect to the provisions of any

---

58 There are also provisions in the RIPA for interception without a warrant, for example where the sender consents or interception is in relation to the provision of services or where regulations are made by the Secretary of States for certain types of interception in the course of certain business, for example in hospitals prisons and in cases of mutual assistance agreements- see sections 3-4 RIPA.

59 Section 6, RIPA

60 Ibid 39 at page 7

61 Ibid 39 at page 7

62 Similar to the words used in Article 8 of the ECHR "necessary measure to safeguard national security"

63 Reflects Article 8 of ECHR "for the prevention of disorder and crime", but is qualified by the word "serious"

international mutual assistance agreement to which it is a party (the 'stated reasons'). The conduct authorised by the interception warrant must be proportionate in the circumstances to what the interception is to achieve and the information sought by the interception must not be reasonably capable of being obtained by other means.

USA

The offence of unlawful interception is found in section 2511 of the US Code, which basically prohibits interception and disclosure of wire, oral, or electronic communications unless otherwise provided for in law.

An application for a Court order for interception under Title III must have the authorisation of either the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General or Acting Assistant Attorney General or a Designated Deputy Assistant Attorney General.[64]

A Court order for interception will be issued only for investigating serious crimes listed in Title III, which includes, among others, bribery, child molestation, extortion, kidnapping, murder, robbery, narcotic offences, crimes against national security and any offence punishable by death or imprisonment for more than one year.[65]

Jamaica

The Interception of Communications Act of Jamaica creates an offence where a person intentionally intercepts a communication in the course of its transmission by means of a telecommunications network offence, except where the communication is intercepted in obedience to a warrant issued by a Judge, the person has reasonable grounds for believing that the person to whom or by whom the communication is transmitted consents to the interception, the communication is intercepted as an ordinary incident to the provision of telecommunications services or to the enforcement of any enactment relating to the use of those services, the communication is not a private communication; the communication is a stored communication and is acquired in accordance with the provisions of any other law, or the interception is of a communication transmitted by a network that is not a public telecommunications network and is done by a person who has a right to control the operation or use of the network, or the express or implied consent of a person.[66]

The offence of unlawful interception carries with it a penalty of a term not exceeding three years or a fine not exceeding three million dollars.

Under Jamaica's Interception of Communications Act, an authorized officer may apply *ex parte* to a Judge in Chambers for a warrant for interception[67]. An authorised officer is defined in the Act to mean the Commissioner of Police, the officer of the Jamaica Constabulary Force in charge of internal security or the National Firearm and Drug Intelligence Centre or any organization replacing the same, or the Chief of Staff, or the head of the Military Intelligence Unit, of the Jamaica Defence Force.[68] Here too these are high level officers who head departments charged with security of the State.

The grounds under which an interception warrant will be issued in Jamaica include national security and the prevention or detection of specified offences including murder, treason, illegal possession of weapons and trafficking of illegal firearms and drugs. The judge must also be satisfied that the information obtained from the interception is likely to assist in investigations concerning national security or the offence and that other investigative procedure have not been or are unlikely to be successful in attaining

---

64 Section 2516 Title III.
65 Ibid.
66 Section 3 Interception of Communications Act , Jamaica.
67 Section 4 Interception of Communication Act, Jamaica.
68 Section 2 Interception of Communications Act , Jamaica.

the information sought to be acquired by means of the warrant or are too dangerous to adopt in the circumstance or having regard to the urgency of the case are impracticable, and it would be in the best interest of the administration of justice to issue the warrant.

Saint Lucia

The Interception of Communications Act of Saint Lucia creates an offence where a person intentionally intercepts a communications in the course of its transmission by means of a postal service or telecommunications network offence except, (like in the case of Jamaica), where the communication is intercepted in obedience to an interception direction or an entry warrant issued by a Judge, the person has reasonable grounds for believing that the person to whom or by whom the communication is transmitted consents to the interception, the communication is stored communication and is acquired in accordance with the provisions of any other law, the communication is intercepted as an ordinary incident to the provision of public postal services or telecommunications services or to the enforcement of any law in force in Saint Lucia relating to the use of those services, the interception is of a communication made through a telecommunications network that is so configured as to render the communication readily accessible to the general public, or the interception is of a communication transmitted by a private telecommunications network and is done by a person who has a right to control the operation or use of the private telecommunications network, or the express or implied consent of the person who has a right to control the operation or use of a private telecommunications network. Additionally, a person does not commit an offence of unlawful interception where the communication is one sent by or intended for a person who has consented to the interception and the person is an authorised officer who believes that the interception of communication is necessary for the purpose of an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health or in the interests of national security[69].

The offence of unlawful interception under the Interception of Communications Act of Saint Lucia carries with it a penalty of a term of imprisonment not exceeding four years or a fine not exceeding twenty thousand dollars.

Under the Saint Lucia Interception of Communications Act, an authorized officer may apply *ex parte* to a Judge in Chambers for an interception direction and/or a warrant for interception[70]. An authorised officer is defined in the Act to mean the Commissioner of Police, the Director of the Financial Intelligence Authority, the Comptroller of Customs, a person for the time being lawfully exercising their functions or authorised in writing to act on their behalf[71]. Again these are the highest level officers charged with security of the State.

The grounds under which an interception direction will be issued in Saint Lucia are in the interests of public order, in the interests of public morality, in the interests of public safety, for the interest of public health, for the prevention or detection of specified offences including blackmail, capital or non-capital murder, manslaughter treason, kidnapping, money laundering and drug trafficking, for the purpose, in circumstances appearing to the judge to be equivalent to those in which he or she would issue an interception direction, or for giving effect to the provisions of any mutual legal assistance agreement. The judge must also be satisfied that other measures have not been or are unlikely to be successful in obtaining the information sought to be acquired by means of the interception direction are too dangerous to adopt in the circumstances, or having regard to the urgency of the case are impracticable and that it would be in the best interests of the administration of justice to issue the interception direction.

ECTEL Member States

---

69 Section 3 Interception of Communications Act , Saint Lucia

70 Section 4 Interception of Communication Act, Saint Lucia

71 Section 2 Interception of Communications Act , Saint Lucia

The Interception of Communications Act of Saint Lucia contains more or less the same provisions of the OECS Model Interception of Communications Bill approved by the Legal Affairs Committee for implementation in the Member States including Antigua and Barbuda, the Commonwealth of Dominica, Grenada, Saint Kitts and Nevis and Saint Vincent and the Grenadines. Coupled with that the Telecommunications Act in all of the ECTEL Member States (which excludes Antigua and Barbuda) creates an offence of unlawful interception of communications by providing that any message transmitted over a public telecommunications network, shall be confidential and shall not be intercepted or interrupted without the consent of the sender, or without a court order made under the Telecommunications Act itself or any other enactment. In Saint Lucia only there is no requirement for a court order once the interception is allowed under the Telecommunications Act or any other enactment. In each case the fine provided is fifteen thousand dollars.[72]

Saint Vincent and the Grenadines Electronic Transactions Act

The Electronic Transactions Act of Saint Vincent and the Grenadines 2007, No.42 creates the offence of illegal interception in the same language of the Model Commonwealth Law on Computer and Computer-related Crime described at paragraph 4.2.1.5.

6.7 Performance of Interception

The scope of an interception warrant is a policy issue which requires determination in the legislative framework. Interception of communications legislation may provide for interception to take place anywhere in a State or within a specified place within a state. Provision is usually made for the interception warrant to be valid for a certain period so that it expires at a specified date. The powers of the interception derived under an interception warrant requires specification in the law so that the boundaries are set for the person executing the interception warrant and any breaches can be adequately taken care of.

Australia

Prior to 13 June 2006, the two modalities of warrants set forth in the TIA Act of Australia were only permitted to authorise interception of communications made to or from telecommunications services that the person is using, or is likely to use. However, the 2006 Act inserted amendments enabling "Equipment-based interception", that is, interception of communications made by means of a particular telecommunications device that a person is using, or is likely to use. These amendments were apposed by some stakeholders who claimed that they appear to have an inappropriately and unjustifiably high potential to result in interception of communications of persons who are not suspects (i.e. are not named in the warrant) because, among other things, the types of device numbers to be used do not necessarily uniquely identify a particular device.)[73]

Interception warrants in Australia may also permit access to stored communications, when such access meets the conditions of the specified exception to the general prohibition on access to stored communications. [74]

Under the TIA Act, a national security warrant is effective for a period not exceeding six months and the Attorney General may revoke a warrant before it expires. On the other hand the duration of a law enforcement warrant must not exceed ninety days[75] and may be extend following the same procedure as the original warrant.

---

72 Section 61 Telecommunications Act Dominica, Section 60 Telecommunications Act Grenada, Section [] Telecommunications Act Saint Kitts and Nevis, Section 61 Telecommunications Act Saint Lucia, Section 59 Telecommunications Act Saint Vincent and the Grenadines.

73 Ibid at pages 6-7.

74 Ibid at page 7.

75 Except if it is a "B-Party" warrant in which case the maximum period in 45 days.

United Kingdom

In the United Kingdom, under the RIPA, the normal warrant used by intercepting agencies is limited to the subject of the interception warrant who is either a person or the premises where the interception is to take place. On the other hand, the certified warrant is exempt from the requirement to specify a subject but requires a certificate by the Secretary of State and is only applied to external communications sent or received outside of the United Kingdom.

Warrants in the United Kingdom are initially valid for a period of six months, whether they are certified or normal. A warrant may be extended, if necessary, on the same grounds as originally granted. Where a warrant is renewed on grounds of serious crime, the extension will be for a further period of six months. In an urgent case, where a warrant is issued by a senior official, a warrant may only be valid for five working days unless the Secretary of State renews it. If a warrant is considered on longer proportionate to or necessary on the ground on which it was granted, it may be cancelled.[76]

USA

Under Title III, an intercepting agency can obtain a court order that does not name a specified telephone line or e-mail account but allows then to tap any phone or internet account that the suspect uses. These are known as “roving traps” and may be granted where there is probable cause to believe that the suspect is attempting to avoid interception from a particular facility for example by switching phones. The Court order may upon the request of the applicant require that third parties, for example, a landlord, provide information facilities and technical assistance which may ne necessary to accomplish the interception unobtrusively with minimum disruption with the services[77]. The order may also require that third parties comply with capability requirements under the CALEA. Under the CALEA, the third parties may be compensated for expenses incurred in providing technical assistance and facilities.

The Court order must “minimize the interception of communications” so that the interception must not continue for any period longer than necessary to achieve the objective of the authorization, nor in any event not for longer than thirty days. Where a court order is renewed the renewal must not exceed thirty days and must be terminated when the object of the order have been achieved.

Jamaica

Under the Interception of Communications Act of Jamaica, a warrant authorizes the interception of communication transmitted by means of a public or private telecommunications network to or from one or more addresses specified in the warrant, being an address or addresses likely to be used for the transmission of communications to or from one particular person specified or described in the warrant or one particular set of premises so specified or described and such other communications, if any, as is necessary to intercept in order to intercept communications within the parameters already set.

The warrant is required to specify the identity, if known, of the person whose communications are to be intercepted, the nature and location of the telecommunications equipment in respect of which interception is authorised, a particular description of the type of communications sought to be intercepted, and, where applicable, a statement of the particular offence to which it relates, the identity of the agency authorized to intercept the communication and the person making the application; and the period for which it is valid.

Where the applicant intends to seek the assistance of any person or entity in implementing the warrant, the Judge on the applicant's request, will direct appropriate persons or entities to furnish information, facilities, or technical assistance necessary to accomplish the interception. The warrant may contain

---

[76] See Ibid 39 at page 8.
[77] Section 2518 Title III.

ancillary provisions as are necessary to secure its implementation. The initial period of validity of a warrant is for the period specified in the warrant not exceeding ninety days, subject to renewal by the Judge in justified circumstances for a period not exceeding ninety days and further renewal for a period not exceeding ninety days in exceptional circumstances. A warrant may be revoked at any time before the expiry the warrant where the warrant is no longer necessary.

Saint Lucia

Under the Interception of Communications Act of Saint Lucia, an interception direction is valid initially for a period of five months (except in cases of urgency where the interception direction is initially for 72 hours), subject to renewal and permits the authorised officer to intercept, at any place in Saint Lucia, any communication in the course of its transmission, to secure the interception in the course of its transmission by means of a postal service or a public or private telecommunications network, of such communications as are described in the interception direction and to secure the disclosure of the intercepted material obtained or required by the interception direction, and of related communications data.

The Interception of Communications Act authorises the interception of communications transmitted by means of a postal service or a public or a private telecommunications network to or from one particular person specified or described in the interception direction, or one particular set of premises so specified and described. The interception direction specifies the identity of the authorised officer on whose behalf an application is made, the person who will execute the interception direction, the name of the person, if known and appropriate, whose communication is to be intercepted and postal service provider or the telecommunications provider to whom the interception direction to intercept must be addressed, if applicable. An interception direction may contain such ancillary provisions as are necessary to secure its implementation and may specify conditions or restrictions relating to the interception of communications authorised in the interception direction.[78]

Under the Interception of Communications Act of Saint Lucia, where an interception direction exists the judge may also grant an entry warrant permitting an authorised officer to enter upon the premises specified in the entry warrant for the purposes of intercepting a postal article or a communication by means of an interception device, installing and maintaining an interception device or removing an interception device. An entry warrant expires when the period or the extended period for which the related interception direction concerned has been issued lapses, it is terminated under by a judge or the interception direction to which it relates is terminated, whichever occurs first. [79]

A judge entitled to issue an interception direction or entry warrant may terminate either the interception direction or the entry warrant or both, if the authorised officer fails to submit a report as required or where the judge upon receipt of the required report is satisfied that the objectives of the interception direction or the entry warrant or both, have been achieved, or the grounds on which the interception direction or the purpose for which the entry warrant was issued, or both has ceased to exist.[80]

6.8 Internal Safeguard Measures

Interception of communications is regarded as a highly intrusive form of investigation which should only be used in limited circumstances, in particular, having regard to the fundamental right to privacy of an individual. In providing a legislative framework for interception, the protection of privacy and the mitigation of the risk of infringement of the right to privacy must be a core consideration. It is therefore necessary that in granting interception powers and in empowering telecommunications providers, law

78 Sections 6 and 7, Interception of Communications Act, Saint Lucia.
79 Section 8, Interception of Communications Act, Saint Lucia.
80 Section 9, Interception of Communications Act, Saint Lucia.

enforcement investigators or intelligence agencies with the capacity and authority to carry on interception of communications activities that care is taken to put measures in place prevent abuse and to respect confidentiality of personal information including lawyer-client confidentiality, customer client confidentiality and doctor-patient confidentiality.

Australia

In Australia, the TIA Act contains important safeguard measures aimed at mitigating the risk of infringement of the right to privacy, namely keeping of registers and restriction on the use or disclosure of intercepted materials.

Registers of Warrants

Under the TIA Act, the Commissioner of the Australian Federal Police (the Commissioner) is required to keep a General Register of Warrants showing the particular details of each law enforcement warrant including the date of issue, the Judge or nominated AAT member who issued the warrant, the agency to which the warrant was issued, the period for which it was or is to be in force, the telecommunications service to which the warrant related, the name of the person likely to use the telecommunications service to which the warrant related and each serious offence in relation to which the judge or nominated AAT member who issued the warrant was satisfied on the application for the warrant. The Commissioner is also required to keep a Special Register of Warrants containing similar particulars as those contained in the General Register for each warrant or renewed warrant that has failed to institute criminal proceedings against a person. The Commissioner is required to submit both the General Register of Warrants and the Special Register of Warrants to the Attorney General every three months for inspection [81].

Restricted use and disclosure of intercepted information

The TIA prohibits intercepted information from being communicated to other persons or from being presented as evidence in legal proceedings except within limited circumstances. The limited circumstances where communication would be allowed include, where the intercepted information is being used in exempt proceedings such as prosecution for prescribed offences namely class 1 and class 2 offences, or being communicated to another person for a permitted purpose including, investigations into class 1 or class 2 offences. In defined circumstances disclosure by particular persons (including, the interceptor, the chief officer of an agency and the members of the police force), may be permitted.[82].

United Kingdom

The RIPA by virtue of section 15 and 16 imposes internal safeguard measures on intercepting agencies with regard to information intercepted under both normal and certified warrants.

Restricted use and disclosure of intercepted information

By virtue of section 15 of the RIPA, it is the duty of the Secretary of State to ensure, in relation to all interception warrants, that such arrangements are in force as he considers necessary for securing that the safeguard measures are satisfied so that the copying, disclosure and retention of intercepted material is limited to the minimum that is necessary for the authorised purposes and the intercepted material and any related communications data and each copy made of any of the material or data (if not destroyed earlier) is destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes. The authorized purposes include the facilitating of the carrying out of the functions of the Secretary of State, the Interception of Communications Commissioner or the Tribunal and to secure fairness in a criminal prosecution.

---

81 Section 81A TIA Act, Australia

82 TIA Act , Australia

In the case of certified warrants extra safeguards are imposed under section 16 so that the Secretary of State must ensure that the intercepted material is read, looked at or listened to by the persons to whom it becomes available by virtue of the warrant to the extent only that it has been certified. Furthermore, in accordance with the Interception of Communications Code of Practice issued by the Home Office in 2002, only appropriately vested persons on the disclosure list of each intercepting agency can have access to intercepted materials or see any report about them.

Exclusion of intercepted materials from legal proceedings

In the United Kingdom intercepted materials are classed as evidence and are generally not admissible in legal proceedings and a party to the proceedings is not allowed to adduced evidence, ask questions, make assertions, make a disclosure or do any other thing for the purposes of or in connection with any legal proceedings which, in any manner, discloses that interception has been permitted. There are however exceptions where for example, a prosecutor needs to review all available materials to ensure that the prosecution is not proceeding unfairly or when the prosecutor has consulted the trial judge who is satisfied that the exceptional circumstances of the case make the disclosure essential in the interests of justice, or in the case of offences relating to interception itself, offences under the Official Secrets Act and non criminal proceedings such as special Immigration Appeals Commission Hearing[83].

The debate in the United Kingdom over whether crime could be fought more effectively by the authorities if the law was amended to provide for the admissibility of intercepted material as evidence in court has been long in the running. The review on use of interception as evidence ordered by the Prime Minister which was completed in 2005 determined that the risks of using intercept evidentially outweighed the benefits of doing so and the impact of new technology needed to be properly considered and factored into the decision-making process. However, a cross party-review known as the Chilcot Review considered the issue again on the basis of the Privy Council. The Home office reports that Government fully endorsed the 2008 Report of the Chilcot Review which concluded that it should be possible to devise a means of proving intercept as evidence in criminal trials in England and Wales – but only providing certain key conditions the report identified can be met and that this would be consistent with the overriding need to protect national security. A work programme was set up to take forward the work identified by the Chilcot Review and included participation by a Cross-Party Advisory Group of Privy Counsellors representing the original Chilcot Team. However, despite detailed examination of potential solutions and extensive work on mitigating the difficulties, the model developed was not legally viable. The Government still wishes to find a way forward. It has agreed further scoping work with the Advisory Group of Privy Counsellors to explore whether a viable approach, building on work to date, can be identified.[84]

Code of Practice

In accordance with section 71 (4), the RIPA, a Code of Practice on Interception of Communications was issued by the Home Office in 2002 under the RIPA (Code of Practice: Interception of Communications Order 2002 and after due public consultation. The Code of Practice specifies the procedures to be followed by public authorities exercising interception powers including those that are empowered to apply for interception warrants and those who may conduct lawful interception of communications with or without warrants. The Code also contains guidelines relating to the execution of warrants and to disclosure, retention and copying of intercepted materials. A person exercising interception powers must have regard to the Code of Practice and it is admissible in evidence in Criminal and civil proceedings although a breach of the Code of Practice itself does not render a person liable to a criminal or civil proceedings.

---

83 Ibid 39 at page 10 and see sections 17 and 18 of the RIPA

84 http://security.homeoffice.gov.uk/ripa/interception/use-interception/index.html

USA

Use of intercepted material

The minimisation procedure required to be implemented by Title III provides a safeguard measure to limit the invasion of privacy. In practice it is reported that law enforcement officers are regarded as satisfying the minimisation obligations by turning of interception equipment when contents outside the scope of the court order are heard and turning it on periodically to determine if communications and content within the scope of the court order are occurring[85].

It is a requirement that intercepted communications must be recorded on tape or other comparable device in order to protect the recording from being edited or altered. On the expiration of the court order the recordings must be immediately made available to the Judge issuing the order and sealed under the judge's directions. The tapes must not be destroyed except upon the order of the issuing or denying judge and must be kept for ten years.[86]

The issuing judge is under an obligation to ensure that, within reasonable time and in any event not later than ninety days, the subject of a court order for interception and other parties as are deemed in the interest of justice are furnished with an inventory including notice of the dates during which the interception activities were carried out and whether the communications were intercepted. The Judge may, upon application, make available to the affected person for inspection portions of the intercepted materials, interception application and court orders[87].

The issuing judge usually requires the intercepting agency to submit reports periodically to show the progress of the interception operation.[88]

Evidential use of intercepted material

Under Title III, sections 2515 and 2518(9) , intercepted materials are admissible as evidence in a court, but each relevant party must be furnished with a copy of the court order for interception and its application not less than ten days before the trial. The ten day period may be waived by the Judge, if he or she finds that the relevant parties will not be unfavoured by the delay in receiving the information.

Jamaica

Use of intercepted materials

Under the Jamaica Interception of Communications Act, a summary offence is created where a person discloses the existence of a warrant or an application for a warrant, other than to a person to whom such disclosure is authorized for the purposes of the Act by virtue of Section 11, a Judge in issuing a warrant shall issue such directions as he considers appropriate for the purpose of requiring the authorized officer to make such arrangements as are necessary for limiting the copying, retention and disclosure of intercepted materials to the minimum that is necessary for the purposes of the investigations in relation to which the warrant was issued or of any prosecution for an offence.

The Jamaica Interception of Communications Act also makes provision for a disclosure order to be issued by a judge where an authorised officer is in possession of protected communication but the key is in the possession of another person and the key is necessary for the purposes of the investigation.

---

85 Ibid 39 at page 24.
86 Section 2518 Title III.
87 Ibid.
88 Ibid 42 at page 24 .

Evidential use of intercepted materials

Under the Jamaica Interception of Communications Act, no details pertaining to the method by which the communication was intercepted or the identity of any party carrying out or assisting in the interception is admissible in evidence in a legal proceeding except where the offence is one under the Act.

Saint Lucia

The Use of Intercepted Materials

The Interception of communications Act in Saint Lucia creates an offence triable on indictment where a person discloses the existence of an application for an interception direction, other than to the authorised officer. [89] By virtue of section 17 the judge in issuing an interception direction or an interception warrant is required to issue it as he considers appropriate to the purpose of requiring the authorised officer to make such arrangements as are necessary for ensuring that regulations relating to disclosure are complied with.[90]Provision is made in the Act for the person to whom the interception direction or an entry warrant, is issued to, as soon as possible after the record has been made, cause to be destroyed after a prescribed period, so much of the record as does not relate directly or indirectly to the purposes for which the interception direction or the entry warrant was issued or is not required for the purposes of any prosecution for an offence.

Evidential Use of Intercepted Materials

The Interception of Communications Act of Saint Lucia makes evidence of interception inadmissible in legal proceedings except in relation to an offence under the interception of communications Act itself or the Telecommunications Act or where the disclosure is of any information that continues to be available as is confined to a disclosure to a person conducting a criminal prosecution for the purpose only of enabling that person to determine what is required of him or her by his or her duty to secure the fairness of the prosecution.[91]

Code of Conduct

By virtue of section 37 of the Interception of Communications Act of Saint Lucia, Interception of Communications (Code of Conduct) Regulations was enacted in 2006 to provide the procedures to be followed authorised and interception officers including procedures relating to use, storage, retention disclosure and dissemination and destruction of intercepted materials. The provisions of this Code of Conduct are in addition to all procedures to be complied with under the Act and an authorised officer who fails to comply with the procedures set out in this Code of Conduct is liable to disciplinary sanctions in addition to all penalties under the Act.

Monitoring Measures

The introduction of monitoring measures in the interception of communications legislative framework is important to ensure implementation and compliance the law and to with reduce the risk of non-compliance or breach of procedures and to prevent abuse of authority and powers conferred by the legislative framework thereby limiting the risk of unlawful interference with the fundamental right to privacy.

---

89 Section 3, Interception of Communications Act, Saint Lucia

90 To date no Regulations have been enacted relating to disclosure of intercepted material in Saint Lucia

91 Section 18 and 19, Interception of Communications Act, Saint Lucia.

Australia

Reporting by the Ombudsman

Under the TIA, the records of the Australian Federal Police and the Australian Crime Commission are to be inspected at least twice during each financial year by the Ombudsman about the in relation to interception and warrants. The purpose of the inspection is to determine the accuracy of entries made both in the General Register of Warrants and the special Register of Warrants and to oversee compliance with the statutory record keeping requirements of the Australian Federal Police and the Australian Crime Commission. In carry out an inspection the Ombudsman has ancillary powers of full access to the records and can enter premises of the Australian Federal Police and the Australian Crime Commission and may require attendance of the head of any one of the agencies to attend a meeting before a specified officer at a specified time or within a specified period and to answer questions that are relevant to the inspection. The Ombudsman is to report the results of the inspection to the Attorney General in writing.

Reporting by the Minister

The Minister of the Crown of each state in Australia is annually required to table an annual report before each House of Parliament. The report is to contain statistics relating to interception including among other things the number of applications for warrants and the number of applications granted, the duration for which warrants are specified to be in force when issued and the actual period for which they are in force [92].

Monitoring by the Legislature

The Australian Parliament has at least one Statutory Committee which monitors interception, namely the Joint Statutory Committee on the Australian Crime Commission established under the Australian Crime Commission Act 2002[93].

United Kingdom

Monitoring by the Interception of Communications Commissioner

The Legislative Framework in the United Kingdom makes provision for the appointment by the Prime Minister of an Interception of Communications Commissioner who must hold or have held high judicial office to oversee the exercise of interception powers. The Commissioner has the responsibility to review the Secretary of State's role in interception warranty, the operation of the regime for acquiring communications data, any notices for requiring the decryption of data authorised by the Secretary of State which relate to intercepted material or communications data and the adequacy of the arrangements made by the Secretary of State for the protection of intercepted material and for the protection of encryption keys for intercepted material and communications data. The Secretary of State is to provide the Interception Commissioner with sufficient technical facilities and staff, after consultation with him.[94]

All persons who may be involved in requesting, authorising, or carrying out, interception are required to cooperate with the Interception Commissioner as he reviews the operation of the regime.[95]

---

92 Sections 99 –103A of the TIA. Act

93 Section 52-55.

94 Section 57, RIPA UK

95 Section 58, RIPA UK.

The Interception of Communications Commissioner is required to report annually to the Prime Minister and that report is laid in Parliament and the parts of it that are not confidential are made available to the public. The Interception of communications Commissioner is also required report to the Prime Minister if he believes that arrangements made by the Secretary of State are inadequate for the protection of either intercepted material or decryption keys.

Monitoring by the Legislature

The Intelligence and Security Committee, which was established under the Intelligence Service Act 1994 is a nine member committee made up of members of the House of Commons and the House of Lords appointed by the Prime Minister, after consultation with the Leader of the Opposition, to oversee the intelligence machinery of the United Kingdom. The Intelligence and Security Committee monitors the expenditure, administration and policies relating to interception of communications conducted by the intelligence services namely MI5, MI6 and GCHQ. The Committee submits an annual report to the Prime Minister which is laid in Parliament and subject to deletion of any part for security reasons. [96]

Monitoring by the public

The RIPA makes provision for the establishment of the Investigatory Powers Tribunal made up of eight senior members of the legal profession appointed by the Queen by Letters Patent. The Tribunal has power to determine its own procedure subject to rules made by the Secretary of State. The Tribunal is to be the appropriate forum for complaints or proceedings against the intelligence services in relation to any proceedings for actions incompatible with the ECHR which are proceedings against any of the intelligence services; or which concern among other thing the use of investigatory powers, any entry on or interference with property, any interference with wireless telegraphy; where any of these take place in relation to conduct by the intelligence services.[97]

USA

Monitoring by the judiciary

The issuing or denying judge must, within thirty days of issuing or refusal to issue a court order for interception, make a report to the Administrative Office of the US Courts. The report must provide the identity of the official applying for the order and the person authorizing the application, the offence under investigation, the type of interception devices and the general location of the devises and the duration of the interception in accordance with the order[98].

Monitoring by the legislature

The Committee on the Judiciary and Intelligence can hold hearings and submit written questions to be addressed by investigative or law enforcement agencies. Interception activities may also be monitored by both the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence. The Committees are responsible for ensuring that resources are not misused and intelligence activities are conducted lawfully.[99]

Each year, in April, the Director of the Administrative Office is required to report to Congress, the number of interception applications and the number of court orders and extension granted or denied during the preceding year together with an analysis of that data.[100]

---

96 Section 10, Intelligence Service Act 1994, c.13.
97 Section 65-69 RIPA.
98 Title III, Section 2519(2).
99 Ibid 39 at page 26.
100 Title III, Section 2519(3)

Monitoring by the public

Public monitoring of interception in the USA takes the form of legal action to suppress the contents of an intercepted communication and any evidence derived from it on grounds such as unlawful interception, interception not done in accordance with the court order or that the court order was insufficient.[101]

Jamaica

The Jamaica interception of Communications Act contains no provision for monitoring.

Saint Lucia

Monitoring by Judiciary

The Interception of communications Act in Saint Lucia provides for a judge who has issued an interception direction or an entry warrant to at the time of issuance or at any stage before the date of expiry of the interception direction or warrant, in writing to require the authorised officer, on whose behalf the relevant application was made in respect of the interception direction or the entry warrant or both, to report to him or her in writing at such intervals as he or she determines on the progress that has been made towards achieving the objectives of the interception direction or the entry warrant and any other matter which the judge deems necessary, or to report on the date of expiry of the entry warrant and interception direction concerned, on whether the interception device has been removed from the premises and, if so, the date of such removal.[102]

Monitoring by the public

A tribunal is established under the Interception of Communications Act of Saint Lucia consisting of judge who is appointed by the Chief Justice acting on his or her own deliberate judgment. The jurisdiction of the Tribunal is established or the purpose of considering and determining complaints made under the Act. The Tribunal has power to regulate its own procedure subject to rules made by the Chief Justice.[103]

Interception capabilities of communications service providers

Australia

In 1997, Australia passed the *Telecommunications Act 1997,* requiring carriers and carriage service providers (telecommunications service providers) to comply with obligations concerning an interception capability and special assistance capability. Under the TIA Act, carriers bear the majority of the capital and ongoing costs for developing and maintaining interception capability.[104]

By virtue of section 31-31D of the TIA Act, the Attorney-General may authorise interception for developing and testing interception capabilities. The Attorney General may upon request authorise interception of communications passing over a telecommunications system by authorised employees of a security authority. The authorisation is subject to a condition prohibiting interception of communications passing over a telecommunications system except for the purposes of development or testing of technologies, or interception capabilities; or communicating, using or recording such communications except for such purposes; and any other conditions specified in the authorisation. The authorisation must be in writing and must specify the period (not exceeding 6 months) for which it will have effect. The head (however described) of the security authority, or a person acting as that head, must ensure that a copy of the authorisation is kept by the authority and is available for inspection on request by the Minister who is responsible for the authority.

---

101 Title III, section 2518(10)(a)

102 Section 12 of the Interception of Communications Act, Saint Lucia.

103 Part V , sections 30 – 33 of the Interception of Communications Act, Saint Lucia

104 http://www.publicsafety.gc.ca/media/bk/2005/bk20051115

Computer networks require testing, monitoring and maintenance to ensure they are not vulnerable to known or predicted security risks and are able to repel or survive an attack. They also require monitoring and maintenance to ensure they operate in an efficient manner, are free of misconfigurations, and that network traffic can travel at optimal speeds. However, some routine network protection activities may inadvertently contravene the TIA Act. Although a number of government agencies are protected by an exemption under the TIA Act, this exemption was only effective until 12 December 2009. This limited timeframe was designed to enable these agencies to undertake network protection activities while a broader solution, applicable to the general community, was developed.

In 2009, the Australian Government approved the release of exposure draft legislation to facilitate public consultation on proposed reforms to the TIA Act. The policy proposal developed by the Attorney General's' Department was set out in the draft TIA (Amendment) Bill 2009 which is aimed at improving the capacity of owners and operators of computer networks to undertake activities to protect their networks.

Saint Lucia

The Interception of communications Act of Saint Lucia provides for the Minister to, declare any electronic, electro magnetic, acoustic, mechanical or other instrument, device or equipment, the design of which renders it primarily useful for purposes of the interception of communications, under the conditions or circumstances specified in the order.[105]

[105] Section 26, Interception of Communications Act, Saint Lucia

Section VII:
Assessment of Regional Texts

7.1 Summary Chart of Status of Beneficiary Countries

Key:

GOOD: There is legislation which adequately addresses the key issues

FAIR: There is some form of reference to the issues in legislation which does not adequately address the key issues

LIMITED: There is reference on the form of policy or consultation document or draft legislation. In case of Bill of Law, "Limited" is the default

NONE: There is no reference in the legislative texts to the key issues

Summary Chart of Status of Beneficiary Countries
International and Regional Trends and Best Practices – Common Key Principles

Country/Region	Legal Mandate	Institutional Framework	Definition of Interception	Right to Intercept	Interception Approval	Confidentiality Measures	Monitoring	Interception Capabilities	Internal Safeguard Measures	Dispute Resolution
Antigua and Barbuda	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED
The Bahamas	NONE	NONE	LIMITED	NONE	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED
Barbados	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE
Belize	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE
Dominica	LIMITED	LIMITED	LIMITED	FAIR	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED
Dominican Republic	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE
Grenada	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED
Guyana	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE
Haiti	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE
Jamaica	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD
St. Kitts and Nevis	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED
Saint Lucia*	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD
St. Vincent and the Grenadines	LIMITED	LIMITED	LIMITED	FAIR	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED
Suriname	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE
Trinidad and Tobago*	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE

7.2 Status of Information and Communications Laws in Beneficiary States

Country	Privacy & Data Protection	Interception of Communications
Antigua and Barbuda		
The Bahamas	Data Protection (Privacy of personal Information Bill http://laws.bahamas.gov.bs/annuals/No3of2003style.html	
Barbados		
Belize		
Commonwealth of Dominica	Privacy and Data Protection Bill www.sfa2005.eu/sites/default/files/Dominica%20Draft%20PRIVACY%20AND%20PERSONAL%20INFORMATION%20BILL%202006.pdf	Interception of Communications Bill (in Parliament)
Dominican Republic		
Grenada	Privacy and Data Protection Bill	Interception of Communications Bill
Guyana		
Haiti		
Jamaica		Interception of Communication Act, Act 5 of 2002, and 18 of 2005 www.moj.gov.jm/laws/statutes/Interception%20of%20Communications%20Act.pdf
Saint Kitts and Nevis	Privacy and Data Protection Bill (in Parliament)	Interception of Communications (in Parliament)
Saint Lucia	Privacy and Data Protection Bill	Interception of Communications Act, No. 31 of 2005
Saint Vincent and the Grenadines	Privacy Act No. 18 of 2003	Draft is existing
Suriname		
Trinidad and Tobago		

Country	Privacy & Data Protection	Interception of Communications
Other related information	www.ictregulationtoolkit.org/en/Section.2107.html www.itu.int/osg/spu/ni/ubiquitous/Presentations/10_lam_dataprotection.pdf http://peterfleischer.blogspot.com/2009/01/launching-another-global-forum-to-talk.html www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_international_standards_en.pdf www.itu-coe.ofta.gov.hk/vtm/ict/faq/q10.htm www.sfa2005.eu/sites/default/files/Malta%20Data%20Protection%20Act.pdf www.oecd.org/document/18/0,2340,en_2649_34255_1815186_119820_1_1_1,00.html	www.itu.int/dms_pub/itu-t/oth/23/01/T23010000060002PDFE.pdf www.itu.int/ITU-T/newslog/New+Report+On+Lawful+Interception.aspx

Section VIII:
Policy Guidelines

The formulation and implementation of policy and legislation on interception of communications law is a controversial issue in many countries, especially because of its intrusive nature vis a vis the fundamental and in many cases the Constitutional right to privacy of personal information. Nevertheless, the importance of interception capabilities to the security and economic and social progress, trade expansion and the well-being of individuals in a country is acknowledged.

It is essential that provision is made for the proper formulation of policy guidelines that reflect clear, common key principles and for the implementation of those policy guidelines as national policy and legislation within the framework for ICT regulation.

Interception of communications policy should therefore be given effect through statements or memoranda of national policy and the enactment of national legislation including primary laws regulations and codes of practice which set the parameters within which the policy must be implemented.

The enactment of legislation is important to ensure lawful authorization, credibility and enforceability of the policy as well as to ensure that there is consistency with national priorities and harmonization as far as possible with regional and international obligations and international best practices and principles.

The same topics used in Section 5 above to frame the overview of Beneficiary Member States' legislation are herein employed as parameters for discussion of policy issues. Therefore, this Section may be helpful for purposes of evidencing the discussions a Beneficiary Member State shall be faced with upon moving from the current status pictured in Section 5 to fill in the gaps detected in Section 6.

8.1 Legal Mandate

- There is a legal mandate/law in place to support or address interception of communications.
- The law gives legislative effect to clear policy guidelines.
- The law reflects common key principles that are in line with international best practices and international and regional obligations.

It is recognised that by its very nature, interception of communications is highly intrusive activity which affects the privacy of an individual. The right to privacy is a fundamental right which is usually protected under the Constitutions of the Beneficiary Countries. It is universally accepted however, that no right is absolute in operation and as long as reasonable grounds exist to limit that right, and that the law is of general application to all citizens, this limitation may be constitutionally acceptable.

Any proposed harmonised national legislation must therefore ensure that the interception of communications as provided therein complies with the provisions of the Constitutions of the Beneficiary Countries. Such legislation must therefore provide for the limitation of the right to privacy in certain circumstances and provide separate frameworks for authorisation, oversight and redress.

International widely accepted parameters, such as the ones contemplated in European Directives 02/58/CE and 06/24/CE, have balanced security and privacy concerns by limiting the latter where a necessary, proportionate and appropriate measure shall be authorized so to protect national security, defence, public security, or to enable prevention, investigation, and persecution of crime. The Court

decisions[106] which have evaluated such parameters are also an important source of consideration, in the same regard, particularly, with respect to terrorism[107].

In some countries, privacy rights applicable over content data, traffic data, and location data are weighted differently, being content data the ones where interception of communication is more intrusive, and therefore, more restricted. There are also different views[108], however, calling attention to the fact that in some circumstances, for instance, in the "navigation" through web sites, traffic data is closely associated with content data, as the address of web sites visited may ensure identification of the contents displayed by such sites.

8.2 Authority Responsible

- There is a relevant government department, agency or regulator responsible for implementing or administering the law.
- There is an authority responsible for authorizing interception of communications.

Interception of communication has criminal, civil, administrative, and labour law implications. As a consequence, a number of authorities are in charge of different aspects of it, in each individual State. For the same reason, some laws rely on other laws or rulings, for instance, the criminal side of interception of communication may depend[109], as criminal norms in blank, upon civil or administrative determination on what are the requirements or formalities which failure to comply with characterizes illegal interception[110].

Therefore, it is important that privacy laws and interception of communication laws are aligned, and not conflicting with each other. And that competent authorities develop joint, coherent strategies and actions.

8.3 Definition of Interception

- The definition of interception is provided in the legislative framework.
- The definition of interception is technology neutral and not confined to any particular communication handling system.
- The definition is broad enough to cover communications sent via various types of networks, e-mail systems and other wireless transmissions.

The definition of interception may serve both the purpose of qualifying legal interception and the purpose of qualifying illegal interception. Hence, such definition shall be carefully worded, in any relevant context.

---

106 For instance, the decision issued by the EC Court of Justice in Feb. 10, 2009, upon Ireland's questioning on EC Directive 06/24. The reasoning adopted therein is similar to the ones which have been adopted by the Interamerican Court of Human Rights in judging cases (330:3801, 306:1892; 316:703) involving privacy rights.

107 The German Supreme Court, which has judged that terrorism shall be seen as an hypothesis which allows for more intrusive mechanisms of surveillance. In the Administrative field, the Council of State, in France, has denied twice the questioning against a decree which has regulated the Law of Jan. 23, 2006 against t terrorism (see "Le Forum des droits sur l'Internet", Rapport d'activité année 2007, Paris, 2008, p. 37)

108 Uicich, Rodolfo D., "El derecho a la intimidad en Internet y en las comunicaciones electrónicas", Buenos Aires, AdHoc, 2009, p. 134.

109 See Jaber, Abbas, "Les infractions commises sur Internet", Paris, L'Harmattan, 2009, p. 58.

110 This is the case, for instance, of Brazilian federal Law 9.296, which Section 10 establishes that to intercept communication without an objective authorized by law is a crime.

Regarding illegal interception of communication, it may be a mean, or an end in itself. That means, it may be an autonomous crime, or it may be an illicit practice absorbed by the typology of other crime, relating to dissemination of informatic viruses, identity theft, or others[111]. It is a matter of policy to define how the illegal interception of communication shall fit in the criminal law system, what shall be the penalties associated to it, the aggravating circumstances, and miscellaneous other aspects.

There are opinions among legal experts in the sense that criminalizing illegal interception of communication must require the element of intent, avoiding that it be extended to situations of mere negligence. There are also opinions in favor of the understanding that criminalizing interception of communication shall not qualify it as a crime of abstract danger[112].

8.4 Effective Framework

- The law provides a framework for authorizing interception of communications which allows for public confidence.
- Unauthorized interception to communications is criminalized in the law.
- The punishment provided in the law is appropriate.

In order to build public confidence on the use of the Internet, cooperation between law enforcement agencies and the private sector must be encouraged, otherwise offenders can take certain measures to complicate the investigations[113].

In addition to using software that enable anonymous communication, the identification can be complicated if the suspect is using public Internet terminals or open wireless networks. Restrictions on the production of software that enable the user to hide his/her identity and on making public Internet access terminals available that do not require identification, could allow law enforcement agencies to conduct investigations more efficiently.

An example of an approach to restrict the use of public terminals to commit criminal offences is Art. 71523 of the Italian Decree 1441524, which was converted into a law in 2005 (Legge No 155/2005). This provision forces anybody who intends to offer public Internet access (e.g. Internet cafes or universities) to apply for authorisation. In addition, the person in question is obliged to request identification from his/her customers prior to giving them access to use the service. With regard to the fact that a private person who sets up a wireless access point is in general not covered by this obligation, monitoring can quite easily be circumvented if the offenders make use of unprotected private networks to hide their identity.

It is questionable whether the extent of improvement in investigations justifies the restriction of access to the Internet and to anonymous communication services. Free access to the Internet is today recognised as an important aspect of the right of free access to information that is protected by the constitution in a number of countries. It is likely that the requirement for identification will affect the use of the Internet as users will then always have to fear that their Internet usage is monitored. Even when the users know that their activities are legal, it can still influence their interaction and usage. At the same time, offenders who want to prevent identification can easily circumvent the identification procedure. They can, for example, use prepaid phone cards bought abroad which do not require identification to access the Internet.

---

111 See Godart, Didier, "Sécurité Informatique – risques, stratégies et solutions", Liège, L. Venanzi, 2005, p. 93-99.

112 Rosende, Eduardo E., "Derecho Penal e Informatica – especial refernecia a las amenazas lógico informáticas", Buenos Aires. Fabián J. Di Plácido, 2008, p. 317.

113 Some comments in this topic were taken from ITU's document "Understanding Cybercrime: a Guide for Developing Countries".

The discard of communication data is another form of building public confidence on the use of the Internet. Provisions such as Sections 5, 6 and 9 of the European Directive 02/58/CE, which impose duties to ISPs so that traffic data and location data are eliminated once no longer necessary or allowed, shall be helpful for achieving public confidence.

In criminalizing unlawful interception of communication, individual Beneficiary Member States must be careful enough to avoid confusion and overlapping between illicit interception and socially acceptable, explicitly or implicitly consented interception. New commercial usages such as feeding electronic marketing with behaviour data of internet users are currently under debate. The frontiers between older, more socially acceptable mechanisms such as *cookies*, and the new ones, such as *web bugs*, seem not clear, so far.

Criminalization of unlawful interception may be affected also by the phenomena of identity theft, a fast-growing misconduct present especially in the Internet, and which has not yet been specifically contemplated in some countries' national legislation[114]. As the obtaining of a third party's identity (sometimes, together with content data) may be accomplished by means of interception of communication[115], it is important to understand the possible connection with those two matters, and develop concerted strategies to face them.

8.5 Interception Authorisation

- The law provides grounds for authorizing interception.
- Provision is made in the law for authorization of the person executing the interception.
- The scope of interception authorisation is specified in the law.
- The legislative framework provides for expiry of an interception authorization.
- The powers of an interception authorisation is specified in the law.
- Provision is made in the law for the person executing the interception direction or warrant to be assisted by any other person.

The possibility to intercept data exchange processes can be important in those cases where law enforcement agencies already know who the communication partners are but have no information about the type of information exchanged. It is important to give them the possibility to record data communication and analyse the content. This includes files downloaded from websites or file-sharing systems, e-mails send or received by the offender and chat conversations.

Definitions of content data, traffic data, and location data, are necessary, as those integrate the category of communication data, subject to interception.

Definitions shall not be too specific nor too broad. An illustrative set of examples, combined with a generic definition, is an adequate combination. Examples of content data which shall be subject to interception may include:

- The content of an e-mail;
- Content on a website that was opened by the suspect;
- The content of a VoIP conversation.

---

[114] See such comment in Uicich, Rodolfo D., "El derecho a la intimidad en Internet y en las comunicaciones electrónicas", Buenos Aires, AdHoc, 2009, p. 89.

[115] See Desgens-Pasanau, Guillaume, and Freyssinet, Éric, "L 'identité à l'ère numérique", Paris, Dalloz, 2009, p. 117.

Provisions on the range of powers which may be authorized by the competent authority shall include reference to remote forensics situations. Given the sensitivity of remote interception as an issue, special focus is given to it in the paragraphs to follow[116].

Search for evidence on the suspect's computer requires physical access to the relevant hardware (computer system and external storage media). This procedure in general goes along with the need to access the apartment, house or office of the suspect. In this case, the suspect will be aware of an ongoing investigation at the same moment when the investigators start carrying out the search. This information could lead to a change in behaviour. If the offender for example attacked some computer systems to test his capabilities in order to participate in the preparation of a much larger series of attacks together with other offenders at a future date, the search procedure could hinder the investigators from identifying the other suspects as it is very likely the offender will stop his communication with them. To avoid the detection of ongoing investigations, law enforcement agencies demand an instrument that allows them to access to computer data stored on the suspect's computes, and that can be secretly used like telephone surveillance for monitoring telephone calls. Such an instrument would enable law enforcement agencies to remotely access the computer of the suspect and search for information.

Currently the question whether or not such instruments are necessary, is intensively discussed. Already in 2001 reports pointed out that the United States FBI was developing a key-logger tool for Internet-related investigations called the "magic lantern". In 2007 reports were published that law enforcement agencies in the United States were using software to trace back suspects that use means of anonymous communication. The reports were referring to a search warrant where the use of a tool called CIPAV was requested. After the Federal Court in Germany decided that the existing Criminal Procedural Law provisions do not allow the investigators to use remote forensic software to secretly search the suspect's computer, a debate about the need to amend the existing laws in this area started. Within the debate information was published that investigation authorities had unlawfully used remote forensic software within a couple of investigations.

Various concepts of "remote forensic software" and especially its possible functions have been discussed.

Seen from a theoretical perspective the software could have the following functions:

- Search function – This function would enable the law enforcement agencies to search for illegal content and collect information about the files stored on the computer1512
- Recording – Investigators could record data that are processed on the computer system of the suspect without being permanently stored. If the suspect for example uses Voice over IP services to communicate with other suspects the content of the conversation would in general not be stored. The remote forensic software could record the processed data to preserve them for the investigators.
- Keylogger – If the remote forensic software contains a module to record the key strokes this module could be used to record passwords that the suspect uses to encrypt files.
- Identification – This function could enable the investigators to prove the participation of the suspect in a criminal offence even if he used anonymous communication services that hinder the investigators to identify the offender by tracing back the IP-address used.
- Activation of peripherals – The remote software could be used to activate a webcam or the microphone for room observation purposes.
- Although the possible functions of the software seem to be very useful for the investigators, it is important to point out that there are a number of legal as well as technical difficulties related to the use of such software. Seen from a technical point of view the following aspects need to be taken into consideration:

---

116 Comments in this topic have extensively taken from ITU's document "Understanding Cybercrime: A Guide for Developing Countries". Reading of the document Is recommended, including the references contained therein in the footnotes, which have not been reproduced herein.

- Difficulties with regard to the installation process – The software needs to be installed on the suspect's computer system. The spread of malicious software proves that the installation of software on the computer of an Internet user without his permission is possible. But the main difference between a virus and a remote forensic software is the fact that the remote forensic software needs to be installed on a specific computer system (the suspect's computer) while a computer virus aims to infect as many computers as possible without need to focus on a specific computer system. There are a number of techniques how the software can be transmitted to the suspect's computer. For example: the installation with physical access to the computer system; placing the software on a website for download; online access to the computer system by circumventing security measures; and, hiding the software in the data stream that is generated during Internet activities, to mention just a few.1517 Due to protection measures such as virus scanners and firewalls that most computers are equipped with, all remote installation methods go along with difficulties for the investigators.
- Advantage of physical access – A number of the analyses conducted (e.g. the physical inspection of data processing media) requires access to the hardware. In addition, the remote forensic software would only enable investigators to analyse computer systems that are connected to the Internet. Furthermore, it is difficult to maintain the integrity of the computer system of the suspect. With regard to these aspects remote forensic software will in general not be able to substitute the physical examination of the suspect's computer system. In addition, a number of legal aspects need to be taken into consideration before implementing a provision that enables the investigators to install remote forensic software. The safeguards established in the Criminal Procedural Codes as well as the Constitutions in many countries limit the potential functions of such software. In addition to the national aspects, the installation of remote forensic software could violate the principle of national sovereignty. If the software is installed on a notebook that is taken out of the country after the installation process, the software might enable the investigators to perform criminal investigations in a foreign territory without the necessary permission of the responsible authorities.

8.6 Secrecy of Intercepted Communications

- The legislative framework provides adequate mechanisms for keeping intercepted communications confidential.
- There are limited exceptions to non-disclosure of intercepted communications provided in the law.

Some countries, such as France[117], have regulated the use of encrypting software to ensure confidentiality of information and of communication. Other countries[118] have used international standards to provide organizational and administrative criteria and best practices, in information security.

8.7 Admissibility as Evidence

- The law does not allow for the fact of interception or the content of intercepted communications to be disclosed in legal proceedings or to be admissible use in evidence.
- The law provides exception to the rule on inadmissibility.

The same concerns which determine confidentiality for storing intercepted communication also apply to non-disclosure. Generally speaking, disclosure is subject to prior Court order. It is advisable that the sharing of confidential, intercepted communication between different authorities, including the ones not in charge of interception or of storage-keeping, be officially regulated.

---

117 See Quéméner, Myryam and Ferry, Joël, "Cybercriminalité – défi mondial et réponses", Paris, Economica, 2007, P. 88.

118 For instance, Brazil, where the Institutional Security Cabinet has followed ISO standards on information security.

Wide acceptance of the theory of the fruit of the poisonous tree, in different countries, emphasizes the importance of appropriate definition and treatment of interception of communication, so that relevant evidence shall be valid, where necessary.

8.8 Equipment with Interception Capabilities

- The legislative framework provides for approval or authorization of equipment with interception capabilities.
- Adequate provision is made in the legislation for protection of the technology.

One of the most important difficulties for investigations based on interception of content data is the use of encryption technology[119]. Given the sensitivity of encryption and decryption as an issue, special focus is given to it in the paragraphs to follow.

The use of encryption technology can enable the offenders to protect the content exchanged in a way that makes it impossible for law enforcement agencies to get access to it. If the victim encrypts the content he transfers, the offenders are only able to intercept the encrypted communication but not analyse the content. Without having access to the key that was used to encrypt the files, a possible decryption could, in the best hypothesis, be feasible but take a very long time.

The use of encryption technology by offenders is a challenge for law enforcement agencies.1484 There are various national and international approaches to address the problem. Due to the different estimates of the threat of encryption technology there is until now no widely accepted international approach to address the topic. The most common solutions are:

- Within criminal investigations law enforcement agencies need to be authorised to break encryption if necessary. Without such authorisation, or having the possibility of issuing a production order, the investigation authorities could be unable to collect the necessary evidence. In addition, or as an option, investigators can be authorised to use key logger software to intercept a passphrase to an encrypted file to break an encryption.
- Regulation that limits the performance of encryption software by restricting the key length. Depending on the degree of the limitation, this would enable the investigators to break the key within a reasonable period of time. Opponents of such a solution fear that the limitations would not only enable investigators to break an encryption but also economic spies that are trying to get access to encrypted business information. In addition, the restriction would only hinder the offender from using a stronger encryption if such software tools would not be available. This would first of all require international standards to prevent the producer of strong encryption products to offer their software in countries without proper restrictions regarding the key length. In any case, the offenders could relatively easily develop their own encryption software that does not limit the key-length.
- The obligation to establish a key escrow system or key recovery procedure for strong encryption products. Implementing such regulations would enable users to continue to use strong encryption technology but enable the investigators to get access to the relevant data by forcing the user to submit the key to special authority that holds the key and provides it to the investigators if necessary. Opponents of such a solution fear that offenders could get access to the submitted keys and with them decrypt secret information. In addition, offenders could relatively easily circumvent the regulation by developing their own encryption software that does not require the submission of the key to the authority.

---

[119] Comments in this topic have extensively taken from ITU's document "Understanding Cybercrime: A Guide for Developing Countries". Reading of the document Is recommended, including the references contained therein in the footnotes, which have not been reproduced herein.

- Another approach is the production order. The term describes the obligation to disclose a key used to encrypt data. The implementation of such instrument was discussed within the 1997 G8 Meeting in Denver. A number of countries have implemented such obligations. One example of national implementation is Sec. 69 of India's Information Technology Act 2000. An example for such obligation is Sec. 49 of the United Kingdom's Regulation of Investigatory Powers Act 2000:

Sec. 49.

(1) This section applies where any protected information

a. *has come into the possession of any person by means of the exercise of a statutory power to seize, detain, inspect, search or otherwise to interfere with documents or other property, or is likely to do so;*

b. *has come into the possession of any person by means of the exercise of any statutory power to intercept communications, or is likely to do so;*

c. *has come into the possession of any person by means of the exercise of any power conferred by an authorisation under section 22(3) or under Part II, or as a result of the giving of a notice under section 22(4), or is likely to do so;*

d. *has come into the possession of any person as a result of having been provided or disclosed in pursuance of any statutory duty (whether or not one arising as a result of a request for information), or is likely to do so; or*

e. *has, by any other lawful means not involving the exercise of statutory powers, come into the possession of any of the intelligence services, the police or the customs and excise, or is likely so to come into the possession of any of those services, the police or the customs and excise.*

(2) If any person with the appropriate permission under Schedule 2 believes, on reasonable grounds-

a. *that a key to the protected information is in the possession of any person,*

b. *that the imposition of a disclosure requirement in respect of the protected information is (i) necessary on grounds falling within subsection (3), or (ii) necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty,*

c. *that the imposition of such a requirement is proportionate to what is sought to be achieved by its imposition, and*

d. *that it is not reasonably practicable for the person with the appropriate permission to obtain possession of the protected information in an intelligible form without the giving of a notice under this section, the person with that permission may, by notice to the person whom he believes to have possession of the key, impose a disclosure requirement in respect of the protected information.*

(3) A disclosure requirement in respect of any protected information is necessary on grounds falling within this subsection if it is necessary-

a. *in the interests of national security;*

b. *for the purpose of preventing or detecting crime; or*

c. *in the interests of the economic well-being of the United Kingdom.*

(4) A notice under this section imposing a disclosure requirement in respect of any protected information-

a. *must be given in writing or (if not in writing) must be given in a manner that produces a record of its having been given;*

b. *must describe the protected information to which the notice relates;*

c. *must specify the matters falling within subsection (2)(b)(i) or (ii) by reference to which the notice is given;*

d. *must specify the office, rank or position held by the person giving it;*

e. *must specify the office, rank or position of the person who for the purposes of Schedule 2 granted permission for the giving of the notice or (if the person giving the notice was entitled to give it without another person's permission) must set out the circumstances in which that entitlement arose;*

f. *must specify the time by which the notice is to be complied with; and*

g. *must set out the disclosure that is required by the notice and the form and manner in which it is to be made; and the time specified for the purposes of paragraph (f) must allow a period for compliance which is reasonable in all the circumstances.*

To ensure that the person obliged to disclosure the key follows the order and actually submits the key, the United Kingdom's Investigatory Powers Act 2000 contains a provision that criminalised the failure to comply with the order.

Sec. 53.

(1) A person to whom a section 49 notice has been given is guilty of an offence if he knowingly fails, in accordance with the notice, to make the disclosure required by virtue of the giving of the notice.

(2) In proceedings against any person for an offence under this section, if it is shown that that person was in possession of a key to any protected information at any time before the time of the giving of the section 49 notice, that person shall be taken for the purposes of those proceedings to have continued to be in possession of that key at all subsequent times, unless it is shown that the key was not in his possession after the giving of the notice and before the time by which he was required to disclose it.

(3) For the purposes of this section a person shall be taken to have shown that he was not in possession of a key to protected information at a particular time if-

a. *sufficient evidence of that fact is adduced to raise an issue with respect to it; and*

b. *the contrary is not proved beyond a reasonable doubt.*

(4) In proceedings against any person for an offence under this section it shall be a defence for that person to show

a. *that it was not reasonably practicable for him to make the disclosure required by virtue of the giving of the section 49 notice before the time by which he was required, in accordance with that notice, to make it; but*

b. *that he did make that disclosure as soon after that time as it was reasonably practicable for him to do so.*

(5) A person guilty of an offence under this section shall be liable-

a. *on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine, or to both;*

b. *on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both.*

The Regulation of Investigatory Powers Act 2006 obliges the suspect of a crime support the work of law enforcement agencies. There are three major concerns related to this regulation:

- A general concern is related to the fact that the obligation leads to a potential conflict with the fundamental rights of a suspect against self-incrimination.1498 Instead of leaving the investigation to the competent authorities the suspect needs to actively support the investigation. The strong protection against self-incrimination in many country raises in so far the question, in how far such regulation has the potential to become a model solution to address the challenge related to encryption technology.
- Another concern is related to the fact that loosing the key could lead to criminal investigation. Although the criminalisation requires that the offender knowingly refuses to disclose the key losing the key could involve people using encryption key in unwanted criminal proceedings. But especially Sec. 53 Subparagraph 2 is potentially interfering with the burden of proof.
- There are technical solutions that enable offenders to circumvent the obligation to disclose the key used to encrypt data. One example how the offender can circumvent the obligation is the use of encryption software based on the "plausible denial ability" principle.

8.9 Internal Safeguard Measures

- Internal safeguard measures are provided for in the law.
- The law provides for monitoring by an independent authority.

Duration of storage-keeping of intercepted communication data shall balance properly security and privacy concerns.

In some countries, a too long term of duration[120] may be seen as unconstitutional.

The independency of the authority in charge of monitoring the existence of appropriate internal safeguards raises the controversial question on where shall the function of interception of communication be allocated to (there are countries which place it within state or federal Police, prosecutor attorneys, special division within the Ministry of Justice, or others).

8.10 Dispute Resolution

- The law makes adequate provision for dispute resolution.
- There is an appropriate body established or designated with adequate powers to deal with dispute resolution.
- Adequate remedies are provided by the legislative framework.

Jurisdiction over globally perpetrated crimes is a controverted matter, subject to different possible views and policy-making. As one of the possible justifications for allowing interception of communication is the investigation of crimes, determining venue has direct effect over determining jurisdiction for granting interception of communication.

The principle of ubiquity – pursuant to which, local laws and local Courts are applicable whenever any portion of a crime is perpetrated within the national territory – has been considered as particularly fit for judging cybercrimes[121].

---

120 In Argentina, Law 25.873, in its Section 2, has adopted the term of 10 years as duration the keeping by ISPs of traffic data and enrollment data of their users, and was found unconstitutional, on Feb. 24, 2009, in the judgment of the so-called "Halabi case". Other countries have much shorter term, at least for the keeping of telephone traffic data (Finland: 3 months; England, Spain, Greece, Denmark, Sweden, and Belgium: 12 months; Italy: 30 months; Ireland: 36 months).

Another important aspect associated with the global dimension of cybercrime is the need of legal provisions regulating extradition, such as, for instance, regulated in the Budapest Convention, of the Council of Europe.

Naturally, the recourse to the principle of ubiquity and the grant of extradition presuppose common understanding on what actions characterize the place of perpetration of the crime, or of a portion of it. Clear criteria in such regard seems advisable, to prevent different views.

The circumstance that the Beneficiary Member States have followed the path of constituting a certain level of economic and legal unification suggests the convenience of deepening the harmonization of criteria of judgment, including by means of setting a common standard of specific legal provisions.

[121] For instance, the Supreme Court of Spain has applied such principle (in an evolutionary process which initially favored the "theory of result") to similar cases (see "Problemática juridical en torno al fenómeno de internet", Consejo General del Poder Judicial, Cuadernos de Derecho Judicial, Madrid, 2000, p. 77/78).

ANNEXES

Annex 1: Bibliography

1. Technical Aspects of Interception (May 2008), ITU, found on www.itu.int/oth/T2301000006/en
2. Communications Assistance for Law Enforcement Act Summary, www.bookrags.com/wiki/Communications_Assistance_for_Law_Enforcement_Act
3. Interception of Communication Act, Act 5 of 2002, and 18 of 2005,
4. www.moj.gov.jm/laws/statutes/Interception%20of%20Comm,unications%20Act.pdf
5. www.itu.int/dms_pub/itu-t/oth/23/01/T23010000060002PDFE.pdf
6. www.itu.int/ITU-T/newslog/New+Report+On+Lawful+Interception.aspxhttp://www.itu.int/ITU
7. The legality of the interception of electronic communications: A concise survey of the principal legal issues and instruments under international, European and national law Working document for the STOA Panel Luxembourg, October 1999, PE 168.184/Vol 4/5 Publisher: European Parliament, Directorate General for Research Author: Prof. Chris Elliot.
8. United Nations Conference on Trade and Development Information Economy Report 2007-2008, Science and technology for development: the new paradigm of ICT Prepared by the UNCTAD secretariat UNITED NATIONS New York and Geneva, 2007
9. ECA/SRO-EA/ICE/AEGM-ICT/2009/03SRO-EA 13th Meeting of the Intergovernmental Committee of Experts (ICE) Mahe, Seychelles, 27-29 April 2009.
10. Harmonisation of the Legal Framework Governing ICTs in West African States, Economic Community of West African States, United Nations Economic Commission for Africa, West African Economic and Monetary Union, by Abdoullah CISSE, University Professor Consultant July 2007.
11. 13th Meeting of the Intergovernmental Committee of Experts (ICE), Mahe, Seychelles, 27-29 April 2009 Ad Hoc Expert Group Meeting: "Harmonization of ICTs Policies and Programmes in Eastern Africa Sub region and Prospects", United Nations Economic Commission for Africa Sub regional Office for Eastern Africa.CA.
12. Cybercrime Legislation Resources, ITU Toolkit for Cybercrime legislation, developed through the American Bar Association's Privacy & Computer Crime Committee Section of Science & Technology Law With Global Participation ICT Applications and Cybersecurity Division Policies and Strategies Department, ITU Telecommunication Development Sector, Draft April 2009.
13. Annex 4 Contribution by Professor Michael Geist University of Ottawa, Faculty of Law, Director of E-commerce Law, Goodmans LLP, found on www.itu.int/ITU-T/special-projects/ip-policy/final/Attach04.doc
14. Uicich, Rodolfo D., "El derecho a la intimidad en Internet y en las comunicaciones electrónicas", Buenos Aires, AdHoc, 2009.
15. Desgens-Pasanau, Guillaume, and Freyssinet, Éric, "L 'identité à l'ère numérique", Paris, Dalloz, 2009.
16. "La criminalité numérique", Institut Nacional des Hautes Études de Securité, Cahiers de la Securité, n. 6, Paris, oct-dec. 2008.

Annex 1

17. "Problemática juridical en torno al fenómeno de internet", Consejo General del Poder Judicial, Cuadernos de Derecho Judicial, Madrid, 2000.

18. "Le Forum des droits sur l'Internet", Rapport d'activité année 2007, Paris, 2008.

19. See Jaber, Abbas, "Les infractions commises sur Internet", Paris, L'Harmattan, 2009.

20. Rosende, Eduardo E., "Derecho Penal e Informatica – especial refernecia a las amenazas lógico informáticas", Buenos Aires. Fabián J. Di Plácido, 2008.

21. Quéméner, Myryam and Ferry, Joël, "Cybercriminalité – défi mondial et réponses", Paris, Economica, 2007

Additional Websites

22. www.ictregulationtoolkit.org/en/Section.2107.html

23. www.itu.int/osg/spu/ni/ubiquitous/Presentations/10_lam_dataprotection.pdf

24. http://peterfleischer.blogspot.com/2009/01/launching-another-global-forum-to-talk.html

25. www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_international_standards_en.pdf

26. www.itu-coe.ofta.gov.hk/vtm/ict/faq/q10.htm

27. www.oecd.org/document/18/0,2340,en_2649_34255_1815186_119820_1_1_1,00.html

28. www.itu.int/dms_pub/itu-t/oth/23/01/T23010000060002PDFE.pdf

29. www.itu.int/ITU-T/newslog/New+Report+On+Lawful+Interception.aspx
www.itu.int/ITU
www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html

Legislative Texts Consulted

30. Saint Lucia Telecommunications (Confidentiality in Network and Services) Regulations No. 17 of 2002

31. Jamaica: Interception of Communications

32. OECS: Interception of Communications Bill

33. Saint Lucia: Privacy and Data Protection Bill No. of 2008

34. Saint Vincent and the Grenadines: Privacy Act, 2003

35. The Bahamas: objects and reasons

36. Saint Lucia: Chapter 3.12 Interception of Communications Act

Annex 2

Participants of the First Consultation Workshop for HIPCAR Project Working Group dealing with ICT Legislative Framework – Information Society Issues
Gros Islet, Saint Lucia, 8-12 March 2010

Officially Designated Participants and Observers

Country	Organization	Last Name	First Name
Antigua and Barbuda	Ministry of Information, Broadcasting, Telecommunications, Science & Technology	SAMUEL	Clement
Bahamas	Utilities Regulation & Competition Authority	DORSETT	Donavon
Barbados	Ministry of Finance, Investment, Telecommunications and Energy	BOURNE	Reginald
Barbados	Ministry of Trade, Industry and Commerce	COPPIN	Chesterfield
Barbados	Cable & Wireless (Barbados) Ltd.	MEDFORD	Glenda E.
Barbados	Ministry of Trade, Industry and Commerce	NICHOLLS	Anthony
Belize	Public Utilities Commission	SMITH	Kingsley
Grenada	National Telecommunications Regulatory Commission	FERGUSON	Ruggles
Grenada	National Telecommunications Regulatory Commission	ROBERTS	Vincent
Guyana	Public Utilities Commission	PERSAUD	Vidiahar
Guyana	Office of the Prime Minister	RAMOTAR	Alexei
Guyana	National Frequency Management Unit	SINGH	Valmikki
Jamaica	University of the West Indies	DUNN	Hopeton S.
Jamaica	LIME	SUTHERLAND CAMPBELL	Melesia
Saint Kitts and Nevis	Ministry of Information and Technology	BOWRIN	Pierre G.
Saint Kitts and Nevis	Ministry of the Attorney General, Justice and Legal Affairs	POWELL WILLIAMS	Tashna
Saint Kitts and Nevis	Ministry of Youth Empowerment, Sports, Information Technology, Telecommunications and Post	WHARTON	Wesley
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	FELICIEN	Barrymore
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	FLOOD	Michael R.
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	JEAN	Allison A.
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	ALEXANDER	K. Andre
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	FRASER	Suenel
Suriname	Telecommunicatie Autoriteit Suriname / Telecommunication Authority Suriname	LETER	Meredith
Suriname	Ministry of Justice and Police, Department of Legislation	SITALDIN	Randhir

Annex 2

Country	Organization	Last Name	First Name
Trinidad and Tobago	Ministry of Public Administration, Legal Services Division	MAHARAJ	Vashti
Trinidad and Tobago	Telecommunications Authority of Trinidad and Tobago	PHILIP	Corinne
Trinidad and Tobago	Ministry of Public Administration, ICT Secretariat	SWIFT	Kevon

Regional / International Organizations' Participants

Organization	Last Name	First Name
Caribbean Community Secretariat (CARICOM)	JOSEPH	Simone
Caribbean ICT Virtual Community (CIVIC)	GEORGE	Gerry
Caribbean ICT Virtual Community (CIVIC)	WILLIAMS	Deirdre
Caribbean Telecommunications Union (CTU)	WILSON	Selby
Delegation of the European Commission to Barbados and the Eastern Caribbean (EC)	HJALMEFJORD	Bo
Eastern Caribbean Telecommunications Authority (ECTEL)	CHARLES	Embert
Eastern Caribbean Telecommunications Authority (ECTEL)	GILCHRIST	John
Eastern Caribbean Telecommunications Authority (ECTEL)	HECTOR	Cheryl
International Telecommunication Union (ITU)	CROSS	Philip
International Telecommunication Union (ITU)	LUDWIG	Kerstin
Office of Trade Negotiations (formerly CRNM) Caribbean Community Secretariat (CARICOM)	BROWNE	Derek E.
Organization of Eastern Caribbean States Secretariat (OECS)	FRANCIS	Karlene

HIPCAR Project Experts

Last Name	First Name
MARTÍNS DE ALMEIDA	Gilberto
GERCKE	Marco
MORGAN[122]	J Paul
PRESCOD	Kwesi

[122] Workshop Chairperson

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

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

Geneva, 2013