Final Report on Proposed Interception of Communications Bill

DRAFT

Grenada

April 2012

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

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.

Please consider the environment before printing this report.

Acknowledgements

The present document – *Final Report on the proposed Interception of Communications Bill 2012 for Grenada* – represents an achievement of the HIPCAR Project "*Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures*", officially launched in Grenada in December 2008. It takes into consideration the vision, mission and general intention of the Government of Grenada as reflected in its information and communications technology (ICT) Strategy and Action Plan 2006-2010.

In response to the challenges and opportunities of ICT's contribution to political, social, economic and environmental development, the International Telecommunication Union (ITU) and the European Commission (EC) joined forces to provide "*Support for the Establishment of Harmonized Policies for the ICT market in the ACP*" – as a component of the "ACP-Information and Communication Technologies (@ACP)" programme financed under the 9th European Development Fund (EDF).

This global ITU-EC-ACP initiative 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 Islands Countries (ICB4PAC).

During its Stage 1, the HIPCAR project prepared Model Legislative Texts and Model Policy Guidelines for the Caribbean encompassing (1) *Information Society issues* (e-Commerce - transactions; electronic evidence; privacy and data protection; interception of communications; cybercrime/e-crimes; and access to public information (freedom of information), and (2) *Telecommunications matters* (universal access/service; interconnection and access; and licensing). In its current Stage 2, HIPCAR is offering in-country assistance upon request to its beneficiary countries in transposing these models into national policies and legislation.

The Government of Grenada has officially requested the project's support in all of the above areas. The current report deals with one of these, namely interception of communications.

Based on the HIPCAR Model Policy Guidelines and Model Legislative Texts developed under Stage 1 of the project, HIPCAR's regional consultant, Ms. Suenel Fraser, drafted the proposed national policy and adapted the bill to Grenada's context based on the feedback received from two national stakeholder consultation workshops. The international consultant, Dr. Marco Gercke, provided some support on the above and facilitated the consultation and capacity building workshops where the documents were reviewed, discussed and adopted by broad consensus at the national stakeholder consultation meetings on cybercrime, interception of communications and e-evidence held in Grenada on 15-16 February 2012 and on 27-30 March 2012.

Grenada's Ministry of ICT served as the local coordinator for the above activities, supported by the local advisor to the HIPCAR National Task Force, Hon. Nazim Burke, Minister of Finance, by the HIPCAR Country Focal Point for Grenada, Ms. Nadica McIntyre, by the ICT Director, Ms. Loretta Simon, by Commissioners and Coordinator at the National Telecommunications Regulatory Commission, Mr. Ruggles Ferguson and Mr. Aldwyn Ferguson respectively, and by Mr. Vincent Roberts, ICT Advisor to the Prime Minister. Grenada's Attorney General, Hon. Rohan Phillips, endorsed the work carried out at the abovementioned consultation workshops.

The production of this report was carried out under the direction of Ms. Kerstin Ludwig, HIPCAR Project Coordinator, and of Mr. Sandro Bazzanella, ITU-EC-ACP Project Manager, with the collaboration of Ms. Tracy Johnson, HIPCAR Project Assistant, and of Ms. Silvia Villar, ITU-EC-ACP Project Assistant. Support was also provided by Mr. Cleveland Thomas, ITU Area Representative for the Caribbean. ITU's Publication Composition Service was responsible for its publication.

Table of Contents

Page

Section I:
Introduction

1.1 This Report

The six (6) HIPCAR[1] model legislative texts provide the project's beneficiary countries with a comprehensive framework to address the most relevant area of regulation with regard to information society issues. They were drafted by reflecting the most current international standards as well as the demands of small and developing countries in general and more specifically, those of HIPCAR's beneficiary countries[2]. The broad involvement of stakeholders from these beneficiary countries in all phases of development of the model legal texts ensures that they can be adopted smoothly and in a timely manner.

The Interception of Communications model will function most effectively with the simultaneous development and passage of a Cybercrime framework, as they are so closely related and dependent on each other to address the concerns of robust regulatory development. In this way there will be optimal opportunity created to utilise the holistic frameworks that are established in the region.

The Interception of Communications Act establishes an appropriate framework that prohibits the illegal interception of communication and defines a narrow window that enables law enforcement to lawfully intercept communication if certain clearly defined conditions are fulfilled.

This report deals with Interception of Communications which considers accepted international and regional best practices and standards, while ensuring compatibility with the prevailing legal system in Grenada. The aim is to meet and respond to the specific requirements of Grenada, taking account of the regional Model Policy Guidelines and Legislative Texts developed under the HIPCAR project.

1.2 The Importance of Effective Policies and Legislation on Interception of Communications

In the context of Information Society, where communications[3] play a significant role, interception of communication – under certain circumstances – has been an essential mechanism in the protection of States and individuals. 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.

---

[1] 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). HIPCAR 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).

[2] The 15 beneficiary countries of the HIPCAR project include Antigua and Barbuda, The Bahamas, Barbados, Belize, The Commonwealth of Dominica, the Dominican Republic, Grenada, Guyana, Haiti, Jamaica, St. Kitts and Nevis, Saint Lucia, St. Vincent and the Grenadines, Suriname, and Trinidad and Tobago.

[3] 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."

In accordance with ITU's Toolkit for Cybercrime Legislation[4], "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..."[5]

Such a definition explains the broad scope of "interception" as well as of the "communication" subject to it, which includes "content" (information communicated) and "traffic"(data relating to communication)[6]. It also outlines different means of communication which may be intercepted. Naturally, Internet-based communication – and especially cybercrime – constitutes an important portion of interception activities from the 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"[7] and of "location data"[8] are of particular interest in this regard.

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 relates to cybersecurity 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, given the increasing sophistication of today's criminals. Lawful interception represents an *indispensable means of gathering information against ruthless criminals.*[9]

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 has failed to keep up with these changes and thus risks degrading 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, Jamaica and most recently St. Kitts and Nevis – to enact legislation that requires electronic communications service providers to be capable of carrying out lawful interception and to regulate interception of communications activities.

---

[4]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.

[5]Section 1 – Definitions, item "k".

[6]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."

[7]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."

[8]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".

[9]Notes on OECS Interception of Communications Bill, page 6 found at http://unpan1.un.org/intradoc/groups/public/documents/TASF/UNPAN024635.pdf

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 communications. 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 labour relationships, privacy rights, or otherwise.

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, remailing techniques, cryptography and steganography are examples of technological means which can be used by criminals that make it hard or even unfeasible to intercept communications or to analyse these. Therefore, the use of such technologies for illicit purposes is a concern.

On the other hand, the required balance between interception requests and privacy rights is another challenge for implementing interception of communications 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 communications is not only a complex legal matter, but also a complicated administrative task.

Different legal systems and different stages of development and implementation of ICT policies represent additional complications for harmonizing national laws. Moreover, countries also have diverse legal and regulatory frameworks in their domestic environments.

Although countries in the Caribbean may be parties to 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 with the European Community.

To take the example of the Member States of the Organization of Eastern Caribbean States (OECS), the Model Interception of Communications Act prepared by the OECS Legislative Drafting Facility in 2003 was approved in that same year by the Legal Affairs Committee – which comprises the Attorneys General (who are directly responsible for implementing the policy on interception) – for enactment in all of the OECS Member States. However, to date, only Saint Lucia in the OECS has enacted an Interception of Communications Act (followed by a similar law in Jamaica) and most recently Saint Kitts and Nevis in 2011.

For further information on the challenges facing the development of policies and legislation relating to interception of communications, Sections 3.2 and 3.3 of ITU's "Understanding Cybercrime: a Guide for Developing Countries"[10] is recommended.

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

Section II:
National Policy and Existing Legislation

2.1 Overview of Existing Legislation

Although Grenada currently has no specific legislation specifically addressing Interception of Communications, neither enacted nor in draft form, the Telecommunications Act No: 31 of 2000, which was enacted in September of 2000, pursuant to section 60 to section 63, prohibits the interception of communications transmitted over a public telecommunications network without the consent of the sender or a court order. The Act also makes it an offence for the telecommunications provider to disclose personal information relating to a subscriber without the consent of that subscriber or a court order.

The Act, however, fails to address the issue of interception of communications over a private network, as well as the procedural requirements for obtaining the required court order. It also does not speak to the parameters within which communications can be legally intercepted.

Despite the existence of this provision, however, it is clear that in order to move towards its goal of an information society and economy, it is necessary for Grenada, to implement more comprehensive legislation, to aid in the fight against cybercrime, as well as to complement cybercrime legislation, consistent with technological advancements.

The Government of Grenada has, therefore, used this opportunity to benefit from the expertise of key stakeholders across the Caribbean region and internationally, who developed Model Policy Guidelines and Legislative text in Interception of Communications, in order to review and modernize its national ICT legislative framework with support under Stage 2 of the HIPCAR Project. This has provided the basis for proposed national policies and legislations which were drafted as a result of the HIPCAR stakeholder consultation workshops held on 15-16 February, 2012 and being endorsed on 27-30 March 2012.

2.2 National ICT Strategy and Action Plan 2006-2010

The ICT Strategy and Action Plan 2006-2010 of Grenada aims at translating "the Vision of the Government of Grenada into a set of policies and actions to enable the exploitation of information and communication technologies as a tool of National development."

In this regard it broadly sets out the regulatory and legislative infrastructure required and lists, *inter alia,* the following objectives:

- To facilitate electronic transactions on a technology neutral basis by means of reliable electronic records;
- To promote public confidence in the validity, integrity and reliability of conducting transactions electronically;
- To promote the development of the legal and business infrastructure necessary to implement electronic transactions securely.

The regulatory policy places emphasis on legislation that is *"technology neutral"* and *"sufficiently flexible to accommodate new technology developments".*

It also requires such legislation to provide a secure legal foundation for the conduct of various forms of electronic transactions including the use of recognition of digital documentation etc.

Under the guidelines set down for the drafting of new legislation, it requires new legislation to cover issues such as the following:

- Recognition of electronic records - evidentiary weight
- Writing
- Original form
- Signatures
- Certification Service Providers
- Formation and validity of contracts and acknowledgement
- Virtual companies
- Encryption
- Liability of intermediaries
- Personal data (Data protection)

Section III:
Stakeholder Consultations

3.1 First Stakeholder Consultation / Capacity Building Workshop

On 15-16 February 2012, the team of consultants, Dr. Marco Gercke, International Consultant, and Regional Consultant Ms. Suenel Fraser, conducted a two day stakeholder consultation workshop, the objective of which was to present a comparative law analysis of the existing legislation in Grenada, the HIPCAR Model legislative Texts and the EGRIP Drafts, on electronic evidence, interception of communications and cybercrime/e-crimes; and to obtain stakeholder input for the finalization of the draft policies and legislations.

The capacity building elements of the workshop also aimed to raise awareness of the updated legal framework and to ensure that roles and responsibilities are clearly articulated for those involved in implementing the legislative frameworks as well as on subjects selected amongst those covered by the updated legal framework.

The workshop was attended by local and regional participants from both the public and private sectors. The participants included representatives from law enforcement, the internet service providers15-16 (ISP's), the media, the Office of the Director of Public Prosecutions, the Legal Drafter from the Attorney General's Office and the Director of Telecommunications and Special Projects, from St. Vincent and the Grenadines as observer. A list of the participants is annexed to this report.

The presentations on Interception of Communications were limited to the HIPCAR Model Legislative Text on Interception of Communications and international best practice, as there was no EGRIP Draft on interception of Communication, nor any specific legislation in Grenada.

The presentations on Interception of Communications attracted few comments from participants. These included a comment by the Observer that governments were concerned that the legislation being drafted vests a government agency with the responsibility for interception. It was however pointed out that this situation already exists in the Telecommunications Act.

One service provider expressed some concern that the proposed Bill did not address situations where an ISP may wish to block some unlawful activity of which they had become aware. It was clarified that interception under the Proposed Bill is purely an investigative tool which allows listening without interrupting. There is also no need to access the particular device. It was clarified that VOIP fell in the realm of cybercrime and as such is not dealt with under interception of communications.

At the commencement of the presentation, it was stated that the interception of communication is reserved for use in serious crimes for example drug trafficking and money laundering, etc.

3.2 Principal Findings

Based on the discussions and comments from the participants and the general tenor of the stakeholder consultation workshop, the HIPCAR Model Legislative Text and Policy Guidelines on Interception of Communications seemed to have gained acceptance as the model text to be transposed into national legislation.

Section IV:
Proposed Interception of Communications Bill 2012

Section IV

4.1 General Overview

The Interception of Communications Bill, hereinafter referred to as "the Bill", introduces a legal framework for the lawful interception of Communications within very definite parameters and at the same time prohibits unlawful interception of communication. It is intended to apply to serious crimes such as drug trafficking and money laundering, etc. as well as to balance the power of the State with individual privacy, while protecting the confidentiality and freedom of information.

The Bill which is based on the HIPCAR Model Legislative Text on Interception of Communications is consistent with international best practice, uses terminology which is technology neutral and broad enough to encompass technological developments and lends itself easily to both regional and international cooperation in the fight against crime. It is divided into nine parts which cover the following:

- Preliminary
- Interception of communications
- Interception equipment
- Disclosure of stored data
- Cost of interception
- Safeguards
- Admissibility of evidence
- Schedule

4.2 Preliminary

This Part of the Bill is divided into three sections namely the "Short Title" which gives the correct name of the Bill, the "Definitions", which provides and explanation of technical and other terms as they are used in the context of the Bill and "Application" which makes it clear that the Bill neither requires nor prohibits the anonymity or encryption of communications, and also limits the application of the Bill to cases where there is no existing legislation already providing for the interception of communications.

4.3 Interception of Communications

This Part prohibits the interception of communications except where it is effected in accordance with the provisions of the Bill, and provides the procedures which must be followed in order to obtain authorisation to effect a lawful interception of communication. It also provides a number of safeguards to prevent the abuse of the power to intercept as well as the privacy of the communications intercepted. In this regard it sets out the criteria on which an application for an interception order will be granted, it limits the duration of the order to a maximum of ninety days, and gives the judge (magistrate) discretion to grant a shorter period. It also empowers the judge (magistrate) to revoke the order in certain circumstances.

4.4 Execution of Interception

This Part sets out the requisite procedures which must be followed in order to effect a lawful interception, after having obtained the necessary authorization. It also establishes the duties and responsibilities of those authorised to execute the interception, for example, the obligation to destroy irrelevant data obtained and to keep confidential all information intercepted. It also imposes a duty on communications services providers to assist an authorised officer in the execution of the order when requested to do so, without incurring any criminal liability.

4.5 Interception Equipment

This Part vests the relevant minister with the power to publish, by Gazette, a list of equipment, devices or instruments, the primary purpose of which is the interception of communications and allows for the submission of comments and representations from individuals. It also prohibits the manufacturing, possession and use of such listed equipment.

4.6 Disclosure of Stored Data

This Part sets out the procedure which must be followed in order to access stored communication data, i.e. data which has already passed transmission and therefore cannot be intercepted such as location data, and takes account of the importance of protecting the privacy of same.

4.7 Cost of Interception

This Part provides that the communication provider must bear the cost of any equipment and maintenance thereof, used for interception.

4.8 Safeguards

This Part recognises and maintains the protection of professional secrecy (doctor/patient; attorney/client) and creates an independent monitoring authority for the purposes of providing guidance and control for the lawful interception of communications, as well as to prevent possible abuse of the powers thereunder.

4.9 Admissibility of Evidence

This Part provides for the admission of evidence obtained via lawful interception while at the same time making inadmissible, evidence obtained through unlawful interception.

4.10 Schedule

The Schedule lists a number of serious crimes for which interception of communications may be employed and empowers the minister to add or delete from same as required, and to make regulations to give effect to the Act.

Section V:
Second Stakeholder Consultation/ Validation Workshop

Section V

5.1 Overview

The Second Grenada-HIPCAR Stakeholder Consultation/Validation Workshop, hosted by the Government of Grenada and co-organized with the National Telecommunications Regulatory Commission and the HIPCAR project, was conducted by the International and Regional Consultants over a four-day period from March 27th to March 30th, 2012.

During this time the Consultants met collectively with participants and representatives from the Ministry of Legal Affairs, the Financial Intelligence Unit (FIU), the Police, the ISPs and the National Telecommunications Regulatory Commission (NTRC).

The Consultants were also featured guests on three live television broadcasts, through which they sought to inform and update the viewing public on the background to the HIPCAR Project, the current status of the Project in Grenada and the benefits of enacting the proposed Bills.

The Consultants also met separately with the legal staff and Permanent Secretary from the Ministry of Legal Affairs, the Police, the Director of Public Prosecutions (DPP), members of the Grenada Cabinet (including the Attorney General) and members of the Opposition.

The feedback from the different groups of stakeholders was very positive. The legal staff of the Ministry of Legal Affairs, the DPP and the Police, were all anxious to know how soon the legislations would be implemented, as they felt that the new legislations would assist them in carrying their functions more effectively, i.e. the investigation and subsequent prosecution of cases and perpetrators respectively.

Both the Grenada Cabinet and the Opposition are also very much supportive of the proposed Bills. As was pointed out by the Leader of the Opposition, the drive towards the greater use of ICTS in the social and economic development of Grenada, commenced under his administration and is being continued under the current administration. Consequently, the Opposition is in no way opposed to the proposed Bills, but rather welcome their implementation, as they are patently aware of the benefits to be derived from their implementation.

Section VI:
Conclusions and Recommendations

6.1 Conclusions

In light of the findings stated in Section III and for the purposes of regional and international harmonization to facilitate regional and international cooperation in combating cybercrime, the proposed Interception of Communications Bill is a necessary part of the legislative framework required for promoting a secure investment environment as well as promoting the confidence of consumers and investors in the security of engaging in electronic commerce.

6.2 Recommendations

The following are recommended:

- Adaptation of the model legislative text on interception of communications to suit the Grenada context;
- National sensitization campaign to raise public awareness of interception of communications and to educate stakeholders and the general public on the provisions of the Act and the types of communications which can be intercepted;
- Training for law enforcement to familiarize same with their duties and procedural requirements under the act;
- Training for law enforcement in the intercepting communication and the handling of the evidence obtained.

Annex 1*:* Interception of Communications Bill

GRENADA
Arrangement of Sections

GRENADA

NO. OF 2012

A BILL to develop a legal framework for the lawful interception of communications and to protect and maintain the right for anonymity, encryption and confidentiality of communications in Grenada.

PART 1 - PRELIMINARY

Short Title

1. This Act may be cited as the Interception of Communications Act, and shall come into force on such date as the Governor-General may appoint by Proclamation published in the *Gazette*.

Definitions

2. (1) "Agency" means a law enforcement agency.

(2) "Authorised officer" means:

a. the Commissioner of Police;

b. the Director of the Financial Intelligence Unit;

c. a person for the time being lawfully exercising the functions of a person stated in paragraph (a) or (b);

d. a person authorised in writing to act on behalf of a person mentioned in paragraphs (a, (b) or (c).

(3) "Communication" means:

a. anything comprising speech, music, sounds, visual images or data of any description, including content data, computer data, traffic data, and/or electronic emissions thereof; or

b. signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus, conveyed across an electronic communication network or any part thereof through the use of any electronic, mechanical, optical, wave, electromechanical, or other device.

(4)"Communications provider" means a person who operates a communications network or who supplies a communications service to more than ten customers.

(5) "Communications network" means any facility or infrastructure used by any person to provide communication services and includes a network whereby a person can send or receive communication services to or from:

a. anywhere in the state;

b. anywhere out of the state.

(6) "Communications service" means any service provided by means of a communications network, whether or not the network is operated by the person providing the service.

(7) "Designated person" means the Minister or any person, prescribed for the purposes of this Act, by the Minister by order published in the Gazette.

(8) "Disclosure order" means an order made pursuant to section 30, requiring access to stored communications data.

(9) "Intercept" means acquiring, viewing, capturing, monitoring or copying of the contents or a portion thereof, of any communication during transmission, through the use of any interception device or method.

(10) "Intercepted communication" means any communication intercepted in the course of its transmission.

(11) "Interception device" means any electronic, mechanical, optical, wave, electromechanical instrument, equipment or apparatus, which is used or can be used, whether by itself or in combination with any other instrument, equipment, programmes or apparatus, to intercept any communication, but does not mean any instrument, equipment or apparatus, or any component thereof:

a. furnished to a customer by a communications provider in the ordinary course of business and being used by the customer in the ordinary course of his or her business;

b. furnished by a customer for connection to the facilities of such communications service and being used by the customer in the ordinary course of business; or

c. being used by a communication provider in the ordinary course of business.

(12) "Interception order" means an authorisation issued pursuant to Section 8.

(13) "Listed equipment" means any equipment declared to be listed equipment pursuant to Section 25, and includes any component of such equipment.

(14) "Minister" means the Minister with responsibility for National Security.

(15) "Stored communications data" means communications that have either not commenced, or have completed, passing over a communications system.

Application

3.(1) Nothing in this Act shall be construed as requiring or prohibiting the anonymity or encryption of communications.

(2) This Act does not apply if interception of communication is provided for under any other law in Grenada

PART 2 - INTERCEPTION OF COMMUNICATIONS

Prohibition of Interception of Communications

4.(1) A person who intentionally and without lawful excuse, intercepts any communication during its transmission commits an offence punishable, on conviction to a fine not exceeding fifty thousand dollars, or by imprisonment for a period not exceeding five years, or both.

(2) A person does not commit an offence under subsection (1), if:

a. The communication is intercepted in accordance with an interception order issued pursuant to Section 8 by a judge (magistrate);

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 communications data 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 communications services or to the enforcement of any law in force relating to the use of those services;

e. The interception is of a communication made through a communications network that is configured so as to render the communication readily accessible to the general public; or

f. The interception is of a communication transmitted and received within an internal network that is used to serve the needs of the company or household and is done by a person who has:

i. a right to control the operation or use of the network; or

ii. 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

b. An authorised officer 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.

Application for the Interception Order

5.(1) An authorised officer or the Director of Public Prosecutions on behalf of an authorised officer, may apply ex- parte to a judge (magistrate) for a order to intercept communications in any case where there are reasonable grounds to believe that the conditions referred to in subsection (1) of Section 8 are satisfied.

(2) Subject to Section 14, an application for the interception order must be in written form and be accompanied by affidavit containing the following:

a. The name of the authorised officer applying or on behalf of whom the application is made;

b. Facts and other grounds on which application is made;

c. The period for which it is requested that the order be in force and shall state why it is considered necessary for the order to be in force for that period;

d. Sufficient information for a judge (magistrate) to issue an interception order on the terms set out in subsection (1) of Section 8;

e. The ground referred to in subsection (1) of Section 8 on which the application is made;

f. Full particulars of all the facts and the circumstances alleged by the authorised officer on whose behalf the application is made including:

i. if practical, a description of the nature and location of the facilities from which, or the premises at which the communication is to be intercepted; and

ii. the basis for believing that evidence relating to the ground on which the application is made will be obtained through the interception;

g. If applicable, whether other investigative procedures have been applied and failed to produce the required evidence or the reason why other investigative procedures reasonably appear to be unlikely to succeed if applied, or are likely to be too dangerous to apply in order to obtain the required evidence;

h. Whether any previous application have been made for the issuing of an interception order in respect of the same person, the same facility or the same premises specified in the application and, if such previous application exists, shall indicate the current status of that application;

i. Any other directives issued by the judge (magistrate).

(3) Where an interception order is applied for on the grounds of national security, the application shall be accompanied by a written authorisation signed by the Minister.

(4) Subject to subsection (5), the records relating to every application for an interception order or the renewal or modification thereof shall be:

a. placed in a packet and sealed by the judge (magistrate) to whom the application is made immediately on determination of the application; and

b. kept in the custody of the court in a place to which the public has no access or such place as the judge (magistrate) may authorise.

(5) The records referred to in subsection (4), may be opened if a judge (magistrate) so orders and then only:

a. for the purpose of dealing with an application for further authorization; or

b. for renewal of an authorization; unless otherwise ordered by the court.

(6) A person who, in an application or affidavit under this Act, makes a statement which he knows to be false in any material particular commits an offence and is liable on summary conviction to a fine not exceeding ten thousand or by imprisonment for a period not exceeding two years, or both.

Application Disclosure

6.(1) Any person who discloses the existence of an Application for an interception order, other than to the authorised officer, commits an offence punishable, on conviction, for a fine not exceeding fifty thousand dollars or by imprisonment for a period not exceeding five years or both.

(2) It shall be a defence in any proceedings against a person to show:

a. that the disclosure was made to an attorney-at-law for the purpose of seeking legal advice;

b. the person to whom, or as the case may be, by whom a disclosure referred to in subsection (1) was made, was the client or a representative of the client.

(3) It shall be a defence in proceedings against a person for an offence under subsection (1) to show that the disclosure was made by an attorney-at-law:

a. in contemplation of, or in connection with any legal proceedings; and

b. for the purposes of the proceedings.

(4) Subsection (2) or subsection (3) shall not apply in the case of a disclosure made in criminal proceedings.

(5) In proceedings against a person for an offence under subsection (1), it shall be a defence for that person to show that the disclosure was confined to a disclosure permitted by the authorised officer.

Issuance of the Interception Order

7.(1) A judge (magistrate) may authorise interception and issue an interception order if he or she is satisfied that:

a. the interception order 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 to believe that such an offence has been, is being or may be committed; or

iii. for the purpose, in circumstances appearing to the judge (magistrate) to be equivalent to those in which he or she would issue an interception order by virtue of sub-paragraph (ii), of giving effect to the provisions of any mutual legal assistance agreement or law:

b. information obtained from the interception is likely to assist in investigations concerning any matter mentioned in paragraph (a), and

c. other procedures:

i. have not been or are unlikely to be successful in obtaining the information sought to be acquired by means of the interception order;

ii. are too dangerous to adopt in the circumstances, or iii. having regard to the urgency of the case are impracticable; and

d. it would be in the best interests of the administration of justice to issue the interception order.

(2) A judge (magistrate) considering the application for the interception order may require an authorised officer to provide further information related to the application as he or she deems necessary.

Scope and Form of Interception Order

8. (1) An interception order shall be issued in writing and shall permit the authorised officer to:

a. intercept communication during its transmission;

b. order a communication provider to intercept the communication during its transmission;

c. execute the interception by means of communication networks or communication service providers as described in the interception order;

d. disclose the intercepted communications obtained or required by the interception order to such persons and in such manner as may be specified in the interception order.

(2) An interception order shall authorise the interception of:

a. communications transmitted by communications networks or providers to or from :

i. a particular individual specified in the interception order;

ii. a particular address specified in the interception order;

b. communications transmitted by communications networks or providers from a particular connection specified in the interception order;

c. such other communication if any as may be necessary in order to intercept communication falling under paragraph (a).

(3) An interception order may authorise entry on any premises specified in the order as referred to in Section 17 for the purpose of installing, maintaining, using or recovering any equipment used to intercept communications specified in the order.

(4) An interception order shall:

a. specify the identity of the authorised officer on whose behalf the application is made;

b. identify the person who will execute the interception order;

c. identify the communications provider to whom an interception order should be addressed and specify if the communications provider shall be authorised to intercept communications, if applicable; and

d. when an interception order authorises the entry on premises under subsection (3):

i. it must specify whether the entry is authorised to be made at any time of the day or night or only during specified hours; ii. it may specify any additional measures that are to be taken to secure and exercise the entry on the premises.

(5) An interception order may contain ancillary provisions that are necessary to secure its implementation in accordance with this Act.

(6) An interception order may specify conditions or restrictions relating to the interception of communications authorised therein.

(7) For the purposes of this section "address" includes premises, email address, telephone number, or any number or designation used for the purpose of identifying communications networks, providers or apparatus.

Duration and Renewal of Interception Warrant

9.(1) An interception order shall be valid for such period, not exceeding 90 days, as the judge (magistrate) shall specify in the order but may be renewed at any time before the end of that period, on an application made pursuant to subsections (3) and (4).

(2) A judge (magistrate) may, on an application for the renewal of an interception order, made by an authorised officer or the Director of Public Prosecutions on behalf of an authorised officer, renew an interception order at any time before the order, (or any current renewal of the order), has expired.

(3) An application for the renewal of an interception order under subsection (2) shall be in writing and shall be accompanied by an affidavit deposing to the circumstances relied on as justifying the renewal of the interception order.

(4) Every application for the renewal of an interception order shall be made in the manner provided by Section 6 and shall give:

a. the reason and period for which the renewal is required; and

b. full particulars, together with times and dates, of any interceptions made or attempted under the order, and an indication of the nature of the information that has been obtained by every such interception.

(5) Every application for the renewal of the interception order shall be supported by such other information as the judge (magistrate) may require.

(6) A renewal of an interception order may be granted under this section if the judge (magistrate) is satisfied that the circumstances referred to in subsection (1) of Section 8 still obtain.

(7) Every renewal of an interception order shall be valid for such period, not exceeding 90 days, as the judge (magistrate) shall specify in the renewal.

(8) If at any time before the end of the periods referred to in subsection (1) and (7) of Section 9, it appears to the authorised officer to whom the order is issued, or a person acting on his or her behalf, that an interception order is no longer necessary, he or she shall make an application to judge (magistrate) for the revocation of the interception order.

Modification of Interception Order

10. (1) A judge (magistrate) may modify any of the provisions of an interception order at any time, after hearing representations from the Authorised officer or the Director of Public Prosecutions acting on behalf of the authorised officer, if he or she is satisfied that there is any change in the circumstances, which may make the requested modifications necessary or expedient.

(2) An application for modification of the interception order shall be made in accordance with Section 6 and shall contain information referred to in subsection (2) of Section 6.

Revocation of Interception Order

11. (1) A judge (magistrate) who issued an interception order or, if he or she is not available, any other judge (magistrate) entitled to issue such a order, may revoke the interception order, if:

a. the authorised officer fails to submit a report in accordance with Section 14, if applicable; or

b. the judge (magistrate) upon receipt of a report submitted pursuant to Section 14 is satisfied that the objectives of the interception order have been achieved; or

c. the grounds on which the interception order was issued have ceased to exist; or

d. the conditions of the application referred to in subsection (1) of Section 7 have changed in a way that an application would not be possible anymore.

(2) Where a judge (magistrate) revokes an interception order pursuant to subsection (1), he or she shall forthwith in writing inform the authorized officer concerned, of the revocation.

(3) If the interception order is revoked, an authorised officer shall, as soon as practicable, after having been informed of the revocation, remove or cause to be removed from the premises to which the interception order relates under subsection (3) of Section 8, any interception device, which was installed under the same subsection.

Consequences of Revocation

12. Where an interception order issued in accordance with this Act is revoked in accordance with Section 12, the contents of any communication intercepted under that order shall be inadmissible as evidence in any criminal proceedings or civil proceedings which may be contemplated unless the Court is of the opinion that the admission of such evidence would not render the trial unfair or otherwise detrimental to the administration of justice.

Urgent Application

13. (1) Where a judge (magistrate) is satisfied that the urgency of the circumstances so requires:

a. He or she may dispense with the requirements for a written application and affidavit and proceed to hear an oral application for an interception order; and

b. If satisfied that an interception order is necessary, he shall issue an interception order in accordance with this Act.

(2) An application under subsection (1) (a) must:

a. contain the information referred to in subsection (2) of Section 6;

b. indicate the particulars of the urgency of the case or the other exceptional circumstances which, in the opinion of the authorized officer justifies the making of an oral application.

(3) A judge (magistrate) may, on an oral application made to him or her, issue an interception order, if he or she is satisfied that:

a. there are reasonable grounds to believe that the interception order shall be issued; and

b. it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, for the authorised officer or the Director of Public Prosecutions applying on behalf of the

authorised officer, to make a written application for the issuing of the interception order, applied for.

(4) Where the judge (magistrate) grants the application for an emergency interception order, the judge (magistrate) shall forthwith make a note in writing of the particulars of the application. The judge (magistrate) shall also make a note of the terms of the order.

(5) An interception order issued on the oral application should have the same scope as it is stated in the Section 9.

(6) Every emergency interception order shall remain valid for 48 hours from the time when it is given, and shall then expire.

(7) Where an interception order is issued under this section, the authorised officer or the Director of Public Prosecutions on behalf of the authorised officer shall within 48 hours of the time of the issue submit to the judge (magistrate) a written application and affidavit in accordance with the provisions of Section 6.

(8) On the expiration of 48 hours from the time of the issue of the interception order; under this section, the judge (magistrate) shall review his or her decision to issue the interception order.

(9) In reviewing his or her decision pursuant to subsection (8), the judge (magistrate) shall determine whether the interception order continues to be necessary pursuant to Section 7.

(10) If the judge (magistrate) is satisfied that the interception order continues to be necessary, he or she shall make an order affirming the issue thereof.

(11) If the judge (magistrate) is not satisfied that an interception order continues to be necessary, he or she shall make an order revoking it.

(12) Where an interception order issued or renewed under this section is revoked under subsection (11), the order shall cease to have effect upon such revocation.

(13) Where the issue of an interception order, is affirmed under subsection (10) of this section, the provisions of section 9 shall apply with respect to its duration as if the date of the order affirming the issue of the interception order were the date on which the order was first issued.

Report on Progress

14. A judge (magistrate) who has issued an interception order, may at the time of issuance thereof, 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 order, to report to him or her in writing on:

a. the progress that has been made towards achieving the objectives of the interception order; and

b. any other matter which the judge (magistrate) considers necessary.

Final Report

15.(1) As soon as practicable after an interception order has expired, the authorised officer who applied for it, shall make a written report to the judge (magistrate) who granted the interception order, or if that judge (magistrate) is unable to act to another judge (magistrate), on the manner in which the power conferred by the interception order has been executed and the results obtained by the execution of that power.

(2) Every report made for the purposes of subsection (1) shall contain the following information:

a. where the interception device was placed;

b. the number of interceptions made by means of the interception device;

c. whether any relevant evidence was obtained by means of the interception device;

d. whether any relevant evidence has been, or is intended to be, used in any criminal proceedings; and

e. whether any records of a communication intercepted pursuant to the interception order have been destroyed in accordance with Section 23 and, if not, why they have not been destroyed.

PART 3 - EXECUTION OF INTERCEPTION

Execution of Interception Order

16. (1) An authorised officer executing an interception order may intercept communications specified in the order and according to the terms of the interception order during their transmission by means of any interception device.

(2) An authorised officer may require a person to intercept communications if specified in the order.

(3) An authorised officer or person, who under an interception order, intercepts or assists in the interception of communications, must take all reasonable steps to minimise the impact of the interception on third parties.

(4) An authorised officer or person acting under or incompliance with an interception order or who aids in good faith, a person whom he believes, on reasonable grounds, is acting in accordance with such authorization, does not incur any criminal or civil liability for anything reasonably donefurther to the interception order.

Execution of Interception Order

17. If an interception order contains permission, on which an authorised officer enters premises, pursuant to subsection (3) Section 8, such authorized officer may, at the time specified in the interception order, enter the premise and perform acts that he or she is authorised to perform in accordance with the interception order.

Duty to Provide Assistance

18. (1) A person who provides communications services shall, if reasonably required, permit and assist, an authorised officer to exercise interception order.

(2) Where the authorised officer intends to order a person to intercept communications, the judge (magistrate) shall oblige the person to execute the interception in compliance with the interception order issued in accordance with subsection (1) of Section 8 or Section 14.

Failure to Assist

19. A person, who intentionally and without lawful excuse Justification, fails to permit or assist an authorised officer in the execution of interception as specified in subsection (1) and (2) of Section 18, commits an offence punishable, on conviction,

to a fine not exceeding fifty thousand dollars or by imprisonment for a period not exceeding five years, or both.

Confidentiality of Intercepted Communication

20. (1) An authorised officer shall make the following arrangements that are necessary to ensure the confidentiality of interception:

a. limit to the minimum that is necessary for the purposes for which the interception order was issued:

i. the extent to which the intercepted communication is disclosed;

ii. the number of persons to whom any of that communication is disclosed;

iii. the extent to which any such communication is copied; and

iv. the number of copies made of any of the communication; and

b. to ensure that each copy made for any of that communication is:

i. stored in a secure manner for so long as its retention is necessary, and

ii. destroyed under the provisions of Section 22.

(2) Any person authorised to intercept communications or provide assistance to the execution of interception shall keep confidential the following information:

a. existence and the contents of the interception order;

b. details of the issue of the interception order and of any renewal or modification of either;

c. existence and the contents of any requirement to provide assistance;

d. steps taken to execute interception order;

e. all intercepted materials with any related communications data.

Failure to Keep Information on Interception Confidential Communication

21. A person who intentionally and without lawful excuse or justification discloses anything that he or she is required to keep confidential under provisions of Section 21, commits an offence punishable, on conviction, to a fine not exceeding Fifty dollars or by imprisonment for a period not exceeding Five years, or both.

Destruction of Records

22.(1) An authorised officer shall ensure that records that are not related to the aim of the interception order are destroyed immediately.

(2) Any records of the information obtained from the interception of communications in pursuance of an interception order, being information that relates wholly or partly and directly or indirectly, to the aim of the interception order, shall be destroyed as soon as it appears that no proceedings, or no further proceedings, will be taken in which the information would be likely to be required to be produced in evidence.

(3) Nothing in subsection (2) shall apply to any record of any information adduced in proceedings in any court.

(4) Every report made to a judge (magistrate) in accordance with section 16 shall state whether or not subsection (2) has yet been complied with, and, if it has not, the judge (magistrate) shall give such directions relating to the eventual destruction of the record as the judge (magistrate) thinks necessary to ensure compliance with that subsection, including a requirement that the judge (magistrate) be advised when the record has been destroyed.

Failure to Destroy Records

23. A person who intentionally and without lawful excuse or justification fails to comply with the requirements of Subsection (1) and (2) of Section 22, commits an offence punishable, on conviction, by imprisonment for a period not exceeding two years, or a fine not exceeding ten thousand dollars, or both.

PART 5- INTERCEPTION EQUIPMENT

Listed Equipment with Interception Capabilities

24.(1) The Minister shall, by notice published in the Gazette, declare any wire, wireless, electronic, optical, magnetic or other instrument, device or equipment, which is primarily designed for purposes of the interception of communications, under the conditions or circumstances specified in the notice, to be listed equipment with interception capabilities.

(2) A notice can be at any time amended or withdrawn.

(3) The first notice under subsection (1) shall be issued by the Minister within three months after the date of commencement of this Act.

(4) Before the Minister exercises the power under subsection (1), the draft of proposed notice shall be published in the Gazette, together with a notice inviting all interested parties within a specified period to submit in writing comments and representations in connection with the proposed notice.

(5) A period of one month shall elapse between the publication of the draft notice and the notice under subsection (1).

(6) Subsection (4) does not apply:

a. if the Minister, in pursuance of comments and representations received in terms of subsection (4) decides to publish a notice referred to in subsection (1) in an amended form;

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.

Prohibition of Manufacture, Possession and Use of Listed Equipment with Interception Capacities

25. (1) Subject to subsection (2) of this section and purchase or use Section27, a person shall not assemble, possess, sell, any listed equipment.

(2) Subsection (1) does not apply in case of authorisation granted under the Section 28.

Without Authorization

26. (1) A person who intentionally and without lawful excuse or justification contravenes or fails to comply with the requirements of Section 25, commits an offence punishable, on conviction, by imprisonment for a period not exceeding three years or a fine not exceeding twenty thousand dollars, or both.

(2) Where any person is convicted of a crime against subsection (1) the court may, as a part of the sentence, order that the equipment with interception capabilities be forfeited.

(3) Where any communications provider, intentionally and without lawful excuse or justification, contravenes or fails to comply with the requirements of Section 25, the Minister or relevant authority may revoke its operating licence.

Authorization to Use Listed Equipment with Interception Capabilities

27.(1) The Minister may, upon application, exempt any person, private body or law enforcement agency from one or all of the prohibited acts listed under subsection (1) of Section 25 for such period and on such conditions as the Minister may determine.

(2) The Minister may only grant an exemption under subsection (1) if he or she is satisfied that:

a. such exemption is in the public interest;

b. the purpose for which the listed equipment will be manufactured, assembled, possessed, sold, purchased or advertised is reasonably necessary; and

c. special circumstances exist which justify such exemption.

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

(4) A certificate of exemption granted under 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; and

b. withdrawal under subsection (5).

PART 5 - DISCLOSURE OF STORED COMMUNICATION DATA

Prohibition of Access to Stored Computer Data

28. (1) Unlawful access to stored communications is prohibited.

(2) A person who intentionally and without lawful excuse or Justification accesses stored communications, or authorises, suffers or permits another person to access a stored communication commits an offence punishable, on conviction, by imprisonment for a period not exceeding three years or a fine not exceeding fifty thousand dollars, or both.

(3) A lawful excuse is given if:

a. stored communication is accessed based on a disclosure order; or

b. stored communication is accessed based on an interception order; or

c. stored communication is accessed based on or under other orders and orders issued in accordance with procedural legislation.

Disclosure of Stored Communication Data

29. (1) Where it appears to the designated person that a person providing communications service is or may be in possession of, or capable of obtaining, any communications data, the designated person may, by disclosure order, require the communications 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 provider is not already in possession of the data, to obtain the data and to disclose the data to an authorised officer.

(2) A judge (magistrate) shall not issue a disclosure order 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 authorized officer.

(3) A judge (magistrate) shall not issue a disclosure order 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 crime or of preventing public disorder;

c. in the interests of public safety;

d. for the purpose of protecting public health;

e. 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.

(4) A disclosure order pursuant to 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 order is issued; and

e. the date on which it is issued.

(5) A disclosure order shall not require;

a. any communications data to be disclosed after the end of the period of one month beginning on the date on which the order 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 communications service, or required to be obtained by him or her, during that period.

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

(7) The disclosure referred to in subsection (6) may be made to:

a. an officer or agent of the service provider, for the purpose of ensuring that the disclosure order is complied with;

b. an attorney-at-law for the purpose of obtaining legal advice or representation in relation to the disclosure order, and a person referred to in paragraph (a) or (b) shall not disclose the existence or operation of the disclosure order, except to the authorized 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 disclosure order, in the case of an officer or agent of the service provider; or

ii. giving legal advice or making representations in relation to the disclosure order, in the case of an attorney-at-law.

Failure to Keep Information on Disclosure Order Confidential

30. A person who intentionally and without lawful excuse or justification discloses anything that he or she is required to keep confidential under subsection (6) of Section 29, commits an offence punishable, on conviction, by imprisonment for a period not exceeding five years, or a fine not exceeding fifty thousand dollars, or both.

PART 6 - COST OF INTERCEPTION

Allocation of Costs

31.(1) Any costs incurred by a communications provider that enables the communications provider to intercept communications and/or store communications, including the investment, technical, maintenance and operating costs must be borne by that communications provider.

PART 7 - SAFEGUARDS

Professional Secrecy

32. If the evidence obtained by the interception of communication, is privileged by virtue of any law protecting:

a. medical secrecy;

b. communications of a professional character between attorney-at-law and a client;

c. bank secrecy;

d. financial secrecy; such evidence shall remain privileged and shall not be given in any court, except with the consent of the person entitled to waive that privilege.

Monitoring of Communications Interception

33.(1) An independent monitoring authority shall be vested with the power to provide guidance and controls in order to make sure that interception of communication is carried out in accordance with legal authorization.

(2) An authorised officer shall, not more than 7 days after submitting a Final Report pursuant to Section 15, submit the following information to the independent monitoring authority for the purpose of keeping a Register of Interception orders:

a. the date of issue of the order;

b. the judge (magistrate) who issued the order;

c. the agency to which the order was issued; and

d. the period for which the order was in force.

(4) The independent monitoring authority:

a. keeps the Register of Interception orders, recording information specified in subsection (2) of Section 33; and

b. submits a report on Monitoring of Communications Interception to the Independent Commissioner on Interception of Communication every 6 months.

(5) The independent monitoring authority may, by written notice given to the chief officer of the relevant authority, require the relevant authority to submit information, which is necessary to make sure that interception of communication is carried out in accordance with this Act.

(6) Where, as a result of monitoring, the independent monitoring authority believes that an authorised officer has violated a provision of this Act, the independent monitoring authority may include this violation into the report on Monitoring of Communications Interception.

Independent Commissioner on Interception of Communications

34.(1) The Independent Commissioner on Interception of Communications shall be appointed by Parliament.

(2) The Independent Commissioner holds office for such period, not exceeding 5 years, as is specified in the instrument of his or her appointment, but is eligible for re-appointment.

(3) The Independent Commissioner for the purposes of an inspection:

a. may, after notifying the chief officer of the agency, enter at any reasonable time premises occupied by the agency; and

b. is entitled to have full and free access at all reasonable times to all records of the agency related to the interception; and

c. is entitled to make copies of, and to take extras from, records of the agency or the Registry of Interception orders; and

d. may require an officer of the agency to give the Independent Commissioner such information as the Registry of Interception orders considers necessary, being information that is in the officer's possession, or to which the officer has access, and that is relevant to the inspection.

(4) The chief officer of an agency shall ensure that the agency's officers provide to the Independent Commissioner such assistance in connection with the performance or exercise of the Independent Commissioner's functions or powers under this Section as the Independent Commissioner reasonably requires.

(5) All requests made by the Independent Commissioner while exercising the duties under subsections (3) and (4) shall be answered in 7days.

(6) Where, as a result of inspection the Independent Commissioner believes that an authorised officer or agency has violated a provision of this Act, the Independent Commissioner may initiate its own investigations on the case.

(7) When as a result of investigations made under subsection (6) the Independent Commissioner discovers any breach of this Act, he or she may issue a binding determination requiring the elimination of the violation or the termination of the activity which contravenes this Act.

(8) The binding determination issued under subsection (7) should be issued in written form and is binding on an authorised officer, agency or private body.

(9) If an authorised officer, agency or private body fails to comply with the requirements of the determination issued under subsection (7) in 14 days after the determination is received, the Independent Commissioner may make an application to the Court to enforce the determination.

(10) An individual or public authority has the right of appeal to the Court against decisions of the Independent Commissioner.

PART 8 - ADMISSIBILITY OF EVIDENCE

Admissibility of Intercepted Communications as Evidence

35. (1) Only communication data intercepted in compliance with this Act shall be admissible as evidence in accordance with the law relating to the admissibility of evidence.

(2) Particulars of a communication intercepted pursuant to an interception order, or an emergency interception order, shall not be received in evidence by any court against any person, unless the party intending to adduce it has given to that person reasonable notice of the party's intention to do so, together with:

a. a transcript of the private communication, where that party intends to adduce it in the form of a recording, or a written statement setting forth the full particulars of the communication, where that party intends to adduce oral evidence of it; and

b. a statement of the time, place (if known), and date of the communication, and of the names and addresses of the parties to the communication, if they are known.

(3) Even if the communication was intercepted under an interception order or an emergency interception order, evidence of a communication intercepted by means of an interception device, or of its substance, meaning, or purport, may not be given in any court unless the evidence relates to the crime specified in the Schedule.

Inadmissibility of Intercepted Communications as Evidence

36. Where a communication, intercepted by means of an interception device, otherwise than in pursuance of an interception order or emergency interception order issued under Section 14, or of any authority conferred by or under any other enactment, has come to the knowledge of a person as a direct or indirect result of that interception or its disclosure, no evidence so acquired of that communication, or of its substance, meaning, or purport, and no other evidence obtained as a direct or indirect result of the interception or disclosure of that communication, shall be given against any person, except in proceedings relating to the unlawful interception of a communication by means of an interception device or the unlawful disclosure of communication unlawfully intercepted in that manner.

PART 9 - SCHEDULE

Amendment of Schedule

37. (1) The Minster may, by order, add to or delete from list of offences contained in the Schedule.

Regulations

38. (1) The minister may make regulations to give effect to the purpose of this Act.

SCHEDULE

(Section 9 (1)(a)(ii))

(1) Murder or Manslaughter or treason.

(2) Kidnapping or abduction.

(3) Money laundering contrary to the Proceeds of Crime Act.

(4) Producing, manufacturing, supplying or otherwise dealing in any dangerous drug in contravention of the Dangerous Drugs Act.

(5) Importing or exporting a dangerous drug in contravention of the Dangerous Drugs Act.

(6) Importation, exportation or trans-shipment of any firearm or ammunition in contravention of the Firearms Act.

(7) Manufacture of, or dealing, in firearms or ammunition in contravention of the Firearms Act.

(8) Illegal possession of a prohibited weapon or any other firearm or ammunition contrary to the Firearms Act.

(9) An offence contrary to the Prevention of Corruption Act.

(10) Arson.

(11) International Convention on hijacking, terrorist offences, etc.

(12) Prevention of Terrorism Act.

(13) Attempting or conspiring to commit, or aiding, abetting, counselling or procuring the commission of, an offence falling within any of the preceding paragraphs.

Explanatory Notes

INTRODUCTION

1. This Act provides a legal framework for the lawful interception of communications. The principal aims of this Act are to prohibit unlawful interception of communications, to define a limited number of

circumstances for authorisation of interception, to establish standards for giving such authorisation and executing it, to balance the power of the state and individual privacy; and to protect confidentiality and freedom of communications.

2. These notes are to explain the content of the Act and need to be read in conjunction with it. They explain the importance of the provisions and, where applicable, reflect the discussions within the HIPCAR[11] Working Group[12] of the First Consultation Workshop of HIPCAR Working Group 1. These notes are not, and are not meant to be, a detailed description of the Act. So where a section or part of a section does not seem to require any comprehensive clarification, comment or reference, or when there was no discussion concerning a particular provision within the working group, no detailed explanation is given.

3. The Act consists of nine parts:

- **Part I** provides definitions and sets the objective of the Act;
- **Part II** prohibits unlawful interception and establishes a limited set of conditions under which interception is deemed to be lawful. It also contains provisions establishing the procedure for obtaining authorisation to intercept communications. Finally, it provides the grounds for granting relevant authorities with the interception order, and the rules for duration, renewal, and revocation of orders;
- **Part III** develops a framework for the execution of interception of communications;
- **Part IV** addresses the issue of prohibition on the equipment with interception capability and suggests the regime for regulating the use of such equipment;
- **Part V** provides recommendations on implementation of the provisions on the disclosure of stored communications data;
- **Part VI** covers the issue of the allocation of costs incurred from interception;
- **Part VII** provides recommendations on safeguards protecting privileged communications and gives the option for implementing monitoring and oversight measures;
- **Part VIII** contains recommendations on the issue of the admissibility of evidences;
- **Part IX** provides a schedule of serious crimes referred to in the Part I of this Act.

COMMENTARY ON SECTIONS

PART I – PRELIMINARY

[11] The full title of the HIPCAR project is *"Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures"*. This 3-year project was launched in September 2008, within the context of an umbrella project embracing the ACP countries funded by the European Union and the International Telecommunication Union. The project is implemented by the International Telecommunication Union (ITU) in collaboration with the Caribbean Community (CARICOM) Secretariat and the Caribbean Telecommunications Union (CTU).

[12] The members of the HIPCAR Working Groups include Ministry and Regulator representatives nominated by their national governments, relevant regional bodies and observers – such as operators and other interested stakeholders. The Terms of Reference for the Working Groups are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/docs/ToR%20HIPCAR%20WGs.pdf.
The Second Consultation Workshop (Stage B) for HIPCAR Working Group 1 on ICT Legislative Framework – Information Society Issues was held in Barbados, 23-26 August 2010. Participants reviewed, discussed and adopted by broad consensus the Draft Model Legislative Text on the respective area of work. Where ever the word "working group" appears in this document, it refers to the aforementioned Workshop.

4. Part I provides preliminary provisions, such as title, definitions, objective and commencement clause.

Section 2. Definitions

5. The definition of "Agency" provided by subsection (1) leaves the determination of the agency or body which will effect interception to the country.

6. The definition for an "authorized officer", was similarly dealt with. While it is very important to determine and define, who will be able to apply for an interception order and will carry out interception procedures, the choice is left to the country, to determine its own list of persons that are granted permission to request an authorisation to intercept communications.

7. Subsection (3) defines what "communication" means for the purposes of constructing a framework that regulates interception. The section is drafted with technology neutrality, and avoids any limitations that could exclude relevant types of communications from the ban on interception. Thus the definition of communications is drafted with the aim to include both *data* and *signals* conveyed across an electronic communication network or any part thereof through the use of any electronic, mechanical, optical, wave, electromechanical, or other device.

8. The definition of **communication provider** in the subsection (4) aims at imposing an obligation to intercept communications. Since this Act makes it possible to oblige operators to intercept communications in accordance with the order, in order to protect small communications providers which are not capable of carrying out an interception, a communications provider is defined as one which provides communications services to more than one hundred customers.

9. There was substantial discussion regarding the definition of **communications network**. First of all, it was discussed whether this definition should include the transmission of information or the provision of communications services. Secondly, it was discussed whether the communications network refers mainly to the services or facilities and infrastructure. Thirdly, the Working Group discussed whether there is a need to provide separate definitions for public and private communications network for the purpose of constructing a framework that regulates interception of communications.

10. It was agreed that a definition of communications network shall be drawn to provide a clear distinction between facilities, infrastructure and services. Thus, the Working Group decided to define communications network as any facility or infrastructure used by any person to provide communication services.

11. Furthermore, it was decided that there is no need to distinguish between public and private networks for the purpose of interception. This is applicable, firstly, to the prohibition on interception: communications shall be protected equally no matter which network they pass through. Moreover, for the purpose of granting power to intercept, identical safeguards and procedures shall be applicable for both types of networks in order to protect equally the rights of individuals using different types of networks. Thus, no distinction is made between public and private communications network for the purposes of this Act.

12. The Working Group also discussed the definition of communications with regard to the scope of the model legislative text. The question was raised whether the model legislative text should regulate the interception of any type of communications, including the postal service, or only electronic communications. Although a lot of participants expressed that postal services and electronic communications shall not be treated differently with regard to interception (e.g. interception should be prohibited, robust safeguards should be implemented), the Working Group agreed that the mandate of the group does not cover the interception of the postal services, hence this Act does not cover the interception of the postal services.

13. The definition of **communication service** provided by subsection (6) is important to make a distinction between communications networks and communications services. It establishes that for the

purpose of this Act, communications service includes a service provided both by the person operating the network and the person who only provides the service without running the network.

14. Definitions of **designated person** and **disclosure order** are provided by subsections (7) and (8) respectively, for the purposes of Part V – disclosure of stored communications data. These definitions shall be included only if the approach suggested by part V is followed and the provisions regulating access to the communications data that either have not commenced or have already passed over a communications network are implemented.

15. Subsection (9) provides one of the main definitions of this Act. In order to determine what is prohibited and regulated by this Act, this subsection establishes that **intercept** means acquiring, viewing, capturing, monitoring or copying of the contents or a portion thereof, of any communication during transmission through the use of any interception device or method. This definition provides two key elements to define what the verb 'intercept' includes. First of all, it comprehends the different actions that can be carried out to intercept, such as viewing, monitoring, copying and capturing. Secondly, it establishes that within the framework of interception all this is applicable only to the communication during its transmission. It was discussed in the working group that since the meaning of interception device is also provided in the legislative text, there is no need to provide detailed explanation for interception device or method within the definition of intercept.

16. Subsection (10) defines **intercepted communication** in order to distinguish it from, for example, stored communications data. Even if communications is stored after the interception is made, the main reason for defining it as intercepted is that it has been captured during its transmission. The definition of intercepted communication is also relevant in order to apply provisions protecting confidentiality of intercepted data and obligations to destroy all records.

17. The definition of **interception device** was designed to include any electronic, mechanical, optical, wave, electromechanical instrument, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, equipment, programmes or apparatus to intercept any communication. There was a discussion at the Consultation Workshop plenary session as to whether the definition of interception device shall include software. It was noted by some of the participants that software can be used to carry out an interception. However, it was agreed that software can not *per se* be used to intercept communications, without hardware, and the definition of interception device covers any type of hardware. Thus, it was agreed that there is no need to include software in this definition.

18. In order to protect normal business activity, subsection (11) excludes any instrument, equipment or apparatus, or any component thereof that is furnished and being used in the ordinary course of operation of business either by customers or by communications providers.

19. Subsection (12) provides the definition for **interception order** by making a reference to Section 8. The main discussion regarding the choice of the term " order" instead of the term "direction" is included to this explanatory report (Section 8).

20. For the purposes of the interception of communications framework, subsection (13) defines what **listed equipment** is. It shall be noted that the term listed equipment is different from interception device. While interception device is a device (including dual-use equipment) which can be used to carry out an interception, listed equipment refers to the special regime developed in order to restrict the use of equipment primarily designed for the purpose of interception. The country is advised to include the definition of listed equipment only if it follows the approach suggested by Section 25 of this Act.

21. The definition of **Minister** is provided for the purposes of defining a Ministry which will develop regulations with regard to the interception of communications. This can for instance be the Ministry of National Security, or any other ministry vested with the power to deal with interception issues.

22. The term **stored communications data** is included in the list of definitions as the distinction between communication during its transmission and communication that either have not commenced, or have completed, passing over a communications system is relevant for drawing a clear line between interception and the disclosure of stored communications data. This Act provides different frameworks for granting capability to intercept communication that is being transmitted and provide access to the stored communications.

Section 3: Application

23. The main purpose of this Section is to determine the scope of this Act, so that nothing in this specific piece of legislation that should be applicable only within the context of interception of communications in the case of serious crimes could be used to restrict the rights of individuals. Subsection (1) thus provides that nothing in this Act shall be construed as requiring or prohibiting the anonymity or encryption of communications. The inclusion of this provision prevents the use of the Act as a basis for a ban on encryption of communications. This does not mean that the legislative text prohibits a beneficiary state to establish such a ban. However, this should be done separately from this piece of legislation.

24. Subsection (1) raised substantial discussions in the Working Group and at the Consultation Workshop plenary session on whether the encryption of communications was a right of individuals, and if such right shall be constrained under the rubric of the interception of communications framework. While policy guidance emphasised that the draft of the model legislative text should not hamper the right of the individual for the anonymity and encryption, some of the Workshop participants raised concerns that the right to encrypt communication may hinder the aim of interception itself. Yet it was highlighted that the prohibition on encryption shall be discussed at a different level since it is not covered by the mandate of the Working Group. However, if the model legislative text does not contain a provision that would restrict the impact of the law to the right for the anonymous and encrypted communications, this legislation could possibly be interpreted as a basis for a ban on encryption. After intensive discussions it was agreed that the explicit restriction of encryption was outside the scope of the model legislative text and that any law based on the model legislative text should not be construed as impacting any right to anonymity or encryption of communications.

25. Subsection (2) makes a distinction between interception of communications under this Act and regulation provided by any other piece of legislation for some specific cases such as interception made by intelligence services. The Working Group agreed that subsection (2) of Section 4 specifies that the model legislative text does not apply if communication is subject to special interception procedures and administrative structures under other law. This means that if there is any other regulation which applies to interception made by intelligence services, or during counter-terrorism activities, or in similar situations, or, as it was pointed out in the Working Group, legislation regarding the interception of postal services exists, this Act does not apply to these special interception procedures.

PART II – INTERCEPTION OF COMMUNICATIONS

26. This part of the Act pursues the main aims of the legislation, namely, to prohibit an unlawful interception of communications and, to establish the limited number of circumstances and strict conditions in which interception can be authorised.

27. The approach on prohibition of interception of communications taken by this Act is similar to many regional and national approaches in this area, such as OECS[13] Model Law, legislation of Australia, Hong

[13] Organisation of Eastern Caribbean States

Kong, South Africa, and the United Kingdom. Criminalisation of unlawful interception in these jurisdictions is usually followed by provisions establishing the lawful excuse for the interception and regulating the authorisation process.

28. All national approaches consider the interception of communications as an exceptional measure that is limited to the investigation of serious crimes. Furthermore, interception requires prior judicial authorisation – mainly by court order, although some countries such as the UK establish the right to intercept without prior court authorisation. Finally, interception can be authorised for a

limited period of time. Following these approaches, in addition to establishing an offence of unlawful interception, this part:

- explains circumstances under which interception is lawful;
- establishes a set of conditions that are necessary to apply for interception orders;
- determines the scope, form and duration of interception order as well as ground for its extension and revocation.

29. Furthermore, this part also provides a number of robust safeguards in order to protect privacy of communications and prevent the abuse of the power to intercept. Every section that grants authorisation for interception is followed by the set of additional restrictions and checks to make sure that interception is necessary and can not be avoided in particular circumstances.

Section 4: Prohibition on Interception of Communications

30. Section 4 creates an offence of unlawful interception and explains the circumstances that can justify the lawfulness of the interception. This approach allows implementing strict safeguards first and then limiting the interception to serious crimes and national security issues.

31. The main purpose of subsection (1) is to protect the privacy of the users of communications services by criminalising interception of any communication during its transmission other than in accordance with the provisions of the Act. Criminalisation of unlawful interception is a necessary measure to protect communications from intrusion. First of all, interception of communications represents a serious infringement on individual privacy which justifies the use of criminal sanctions. Prohibiting interception of communications by means of criminal sanction ensures that the victim will obtain assistance from law enforcement agencies in identifying the source of criminal conduct. Furthermore, the victim has no remedy in civil law if the interception of communications was carried out with unauthorised entry into private premises. Finally, criminalisation of the unlawful interception also meets the reasonable expectations of the communications' parties to the communication: any intrusion should be prohibited unless authorised in compliance with law.

32. Subsection (2) specifies the set of certain narrow exceptions. This set of exclusions is very important to secure that interception can be lawful when it is authorised and to justify the interception in certain cases when judicial authorisation is not necessary.

33. Subsection (2) (a) orders the right to intercept in accordance with the authorisation obtained in court. This Act regulates the process of obtaining and executing such an authorisation.

34. Subsection (2) (b) makes interception lawful when there are reasonable grounds to believe that the party to a communication has given consent for it. This provision is important to exclude consensual interception from the scope of the Act. This model Act focuses on situations where the parties of the communication do not agree to the interception because only in this case the interception interferes with the right to privacy. There is no interception if the parties agree to it. Most of the existing approaches do not regulate consensual interception and participant monitoring of communications because the right to intercept one's own communications protects private interest of the person, particularly in the commercial and business context. A party to communication shall take the risk of

disclosure of communication by another party. Furthermore, the right of the party to take accurate notes of a conversation and then reproduce these notes might correspond to the right to wiretap one's own communications as known in some jurisdictions.

35. Subsection (2) (c) excludes stored communications data acquired under or by virtue of any other law. This provision makes a clear distinction between interception – capturing communications during their transmission – and acquiring of stored communications data that is not commenced or has completed passing through communications network.

36. Subsection (2) (d) makes it lawful to intercept communication as an ordinary incident to the provision of communications services or to the enforcement of any law in force in relation to the use of those services. This exemption is crucial to secure the regular commercial activity of communications operators. For example, communications service providers may be required to detect and eliminate radio interference and to ensure compliance with the licensing conditions or to make tests and measurements of communications apparatus to determine whether it complies with the requirements under the regulations or the conditions of the licence under which it is held. This may include interceptions. As these interceptions are necessary to assure that the telecommunication system is working properly, interceptions for these purposes are exempted from criminalization under this Act.

37. Furthermore, communication service operators may have a duty to maintain the quality of service provided in communications network. They may also be under an obligation to comply with conditions of the licence. For example, they have to conduct interceptions in order to ensure that noise in the communications network is maintained at an acceptable level. Thus, service operators should also be permitted to intercept telecommunications for the purpose of providing telecommunication service or carrying out mechanical or service quality control checks. Subsection (2) (d) protects this right.

38. Subsection (2) (e) limits the criminalisation with regard to the interception of a communication made through a communications network that is configured in a way to render the communication readily accessible to the general public. This is important to protect the person intercepting communications which are not initially safeguarded by privacy rights, since they are readily accessible to the public.

39. Subsection (2) (f) makes an exemption for interception of communications received and transmitted within a network which serves the need of a private company or household if the interception is done by the person that has a right to control the operation or use of the network or with express or implied consent of such a person. This provision is particularly relevant for a person with the right to control a communications network within the company or household and allows intercepting their own networks without committing an offence. This can include, for instance, monitoring telephone calls using a second handset in a house, or recording customer calls in banks in order to retain the record of transactions, recording calls to customer service in big companies, etc.

40. The Working Group discussed whether it is necessary to define 'network' referred to in the Subsection (2) (f) as a private network and include the definition into the Preliminary Part of the model legislative text. It was agreed that there is no reason to distinguish between public and private networks with regard to the interception. A person using a communications network has the right to be protected from unlawful interception, irrespective of whether the network is public or private. Communications should be safeguarded from interception in both networks. The Working Group decided to define the internal company networks and household networks only in this subsection for the purpose of this provision.

41. Subsection (3) provides an additional set of exceptions. Based on Subsection (3) (a) interception of communication sent by or intended for a person, who has given consent for the interception is considered lawful. This provision follows the approach of excluding consensual interception from criminalisation. The difference between Subsections (2) (b) and Subsection (3) (a) is that the latter covers the case when consent has been clearly expressed.

42. Subsection (3) (b) provides a lawful excuse for the interception made in the case of emergency. This provision is important to secure the right to take all reasonable measures to prevent 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 when there is no possibility to apply for authorisation in advance. However, it should be specially emphasized that this provision covers only cases of real urgency.

Section 5. Application for the Interception Order

43. Section 5 establishes the procedure for the initial application to authorise interception.

44. Subsection (1) provides that an authorised officer may apply *ex parte* to a judge (magistrate) for a order to intercept communications in any case where there are reasonable grounds to believe that the conditions for the issuance of the interception order are fulfilled. This provision contains several important implications for the procedure of the authorisation of the interception: (1) interception is granted under the order system; (2) interception shall be authorised by court; (3) application is made '*ex parte'*.

45. The order system is an essential conventional mechanism adopted by many countries in sanctioning intrusions such as entry and search of premises and interception of communications. It has several advantages. Firstly, it entails approval by an independent authority before the interception takes place. Secondly, it provides the intruder with a written permission which he or she can produce only under certain conditions. Furthermore, a order system is especially important when the intrusion requires the technical assistance of a third party. This is the usual situation when interception of communications is carried out by communication networks upon order by a court. Finally, the order system has advantages in cases where physical intrusion into premises is involved.

46. When the intrusion requires no external assistance and no entry to premises, the importance of the order is determined by the seriousness of such intrusion as interception of communications. If the order system is implemented only for some types of the interception, it may encourage use of interception activities outside the order requirement. To implement an integrated approach, this Act requires an authorised officer to apply for an order in any case when interception is considered necessary.

47. This section introduces the term 'interception order' with regard to authorisation to intercept communications. The Working Group raised the issue of the use of the term 'order' instead of the term 'direction'. It was agreed that although both options are possible, the term 'order' is preferable for the scope of the model legislative text, (on which this Act is based), as it covers the cases where authorisation to enter on premises is necessary. Courts may include a special entry clause in the order. If the court issues an 'interception direction' instead there is a need to issue the additional entry order. Thus, the term 'interception order' is used for the purposes of this Act.

48. The issue of authorisation by the court is very important because the additional independence afforded by a judicial determination provides necessary checks and balances to the seriousness of intrusion. According to the model legislative text, all orders sanctioning interception shall be authorised only by the courts, with no distinction made between orders relating to law enforcement and those relating to national security. Although some countries distinguish between orders according to whether they relate to crime (for the judiciary) or public security (for the executive), the comprehensive approach which strikes a balance between the public interest and the rights of the individual is to require that all authorisations are made by court.

49. The implementation of the requirement to authorise interception by court is important to keep the balance with regard to the rights of the individual and the interests of state. It is essential for maintaining public confidence in the system that there is an independent approval of the actions in such a sensitive area as interception of communications. That may not be achieved by allowing high public officials to approve applications made by another part of the administration. The best way to ensure the efficiency of checks and balances is to introduce a judge (magistrate) as an independent arbiter of the

necessity of interception. Judicial involvement in the process of granting authorisation to intercept will ensure that an authorised officer applying for the order will have to consider the matter carefully. It will also decrease the possibility of the abuse of power.

50. With regard to the application process, subsection 6 (1) requires that the application be made ex parte. This enables an authorised officer to apply for the interception order based entirely on evidence presented by him or her without notifying the person whose communications shall be intercepted.

51. There was also a substantial discussion in the Working Group on the eligibility of the authorized officer to apply for the interception order. Many national approaches including regional bills (such as the OECS Model Law on Interception of Communications) require that the application is submitted by the Director of Public Prosecution on the behalf of the authorised officer, to provide an additional mechanism of checks and balances. However, participants of the working group expressed the opinion that countries, depending on their national legal traditions, should be given an option to allow an authorised officer to apply without turning to the Director of Public Prosecutions. It was agreed that each country should have this option while implementing interception legislation. It is therefore up to country to decide if the application shall be made by an Authorised Officer or by Director of Public Prosecution on behalf of the authorised officer.

52. Subsection (2) of Section 6 provides that an application for an interception order must be in written form and be accompanied by affidavit specifying the circumstances in which such request is made. The aim of this Subsection is to establish the requirements for the form of the application and provide a set of requirements that each application shall meet. This is necessary to ensure that the process of application for the authorisation follows the specific requirements and, since all documents must be provided in written form, to guarantee the transparency of the application process.

53. According to subsection (2) (a)-(i), applications must be made in writing and give reasons for the authorisation of interception. This provision assures that a factual basis for granting the interception order is provided. Interception may cover only the specific suspect or presumed contact persons. Written application accompanied by affidavit guarantees that “exploratory” or general interception will not be permitted.

54. The form of supporting evidence (affidavit) was intensively discussed. Most national approaches require prior authorisation of a court in order to initiate the interception of communications. However, the process of application differs from jurisdiction to jurisdiction. Although a majority of countries agree that applications need to be submitted in written form, the standards regarding supporting evidence vary significantly. Some countries require that evidence in presented in form of a sworn written statement (Canada, the USA, Australia, OECS Model Law) while other jurisdictions follow the approach of hearing viva voce evidence representation (e.g. Denmark, Finland, Slovenia).

55. Subsection (2) of Section 6 is based on submitting supporting evidence in writing. This model was selected by the Working Group, firstly, because it was widely implemented in common law countries. Secondly, provisions requiring the submission of written statements have been implemented due to the possible difference in regulating the recording and transcription of the viva voce evidence. Obligation to submit supporting evidence in writing is a necessary measure to ensure the transparency of applications and to prevent the opportunity for abuse.

56. In order to enable a court to make an informed decision as to whether or not a order shall be issued, subsections (2) (a) – (2)(i) oblige an authorised officer to provide the court with information showing that interception is necessary for the intended purpose. To guarantee that interception is granted only for a particular case, legislation includes the requirement to present detailed affidavit, containing all the particulars of the case, including facts and other grounds on which the application submitted; period for which it is requested that the order be in force; the basis for believing that evidence relating to the ground on which the application is made will be obtained through the interception. Moreover, the requirement of subsection (2) (g) highlights the need to provide justification for the interception as ‘last resort’ measure. This subsection requires providing the details of the difficulties which would have

arisen if the investigation is restricted to conventional methods or why conventional methods have failed.

57. Subsection (3) provides the additional requirements for the case when application is made on the ground of national security. In this case, it should be accompanied by a written authorisation signed by the Minister. This provision is intended to secure that the particulars of the case related to national security is provided to the court.

58. In order to develop safeguards for the confidentiality of the application for the interception order, Subsections (4) and (5) introduce a set of measures to restrict access to the application for interception order. They establish the requirements for the confidentiality of the application and procedures assuring non-disclosure of the application information. This is important because the handling of applications and the management of files by the court may give rise to problems in maintaining the confidentiality of information during the application process if the access to the application is not restricted to a certain number of officials. The court should ensure that all documents relating to applications for orders are kept in safe custody. It is essential that such documents (including the orders themselves) are kept confidential. The whole concept of interception as a hidden investigation could be undermined if any information concerning the applications is divulged.

59. The Working Group decided to add an additional provision to the Section 6 – subsection (6) criminalising false statement knowingly made by the person in the application for the interception order or affidavit. This provision is a safeguard to prevent the possible abuse that arises from the ex parte application process when the decision of the judge (magistrate) is based entirely on the evidence submitted by the applicant. The person whose communications are to be intercepted has no opportunity to question supporting evidence at the time of the application. Thus, when an authorised officer swears the affidavits, he or she shall be subject to prosecution if false evidence is knowingly provided.

Section 6. Application Disclosure

60. To protect the secrecy of the investigation and to provide a safeguard for the confidentiality of the application, Section 6 criminalises the disclosure of the existence of the application for the interception order. This criminalisation is necessary because deliberate breach of security of the application could lead to a conspiracy to undermine the investigation and hamper the administration of justice.

61. However, to maintain the balance and to protect the right of any person to seek legal advice, subsections (2) and (3) make an exemption from the scope of criminalisation with regard to disclosure made to an attorney-at-law.

Section 7. The Issuance of the Interception Order

62. The aim of this section is to provide the framework for granting an authorisation to intercept communications after applying for an interception order. Since the approach is to restrict the power to intercept to a limited number of circumstances, this section ensures that robust safeguards are in place and the judge (magistrate) is satisfied with the necessity of carrying out interception.

63. As a safeguard against the power to intercept communications, Subsection (1) establishes a set of circumstances that shall be analysed and confirmed by a judge (magistrate) before the issuance of the interception order. The first set of requirements provided by subsection (1) (a) (i), (ii), (iii) is related to the nature of the criminal activity that justifies the authorisation to intercept. A judge (magistrate) authorising the interception shall be satisfied that obtaining the information is necessary in the interests of national security or for the prevention or detection of a particular serious crime, including the cases of mutual legal assistance, or information obtained from the interception is likely to assist in investigations concerning any matter mentioned above.

64. National security – subsection (1) (a) (i) represents a particular ground for the infringement of person's right to the privacy of communication. This ground for granting authorisation to intercept may raise the question of balancing state interests and individual privacy. The freedom from interference with privacy is not absolute, since it must be set against competing public interests. Limitation of this freedom must be necessary for the exercise of the competing interests and national security is one of them. The requirement for court authorisation can provide the balance and prevent the abuse of the interception on the ground of national security.

65. Subsection (1) (a) (ii) provides the second ground for granting an interception order: prevention or detection of any offence specified in the Schedule, where there are reasonable grounds to believe that such an offence has been, is being or may be committed. This subsection refers to the Schedule that is introduced to establish the set of particular serious crimes justifying an interception. The guiding principle for implementing this provision is that the means of investigation must be proportionate to the gravity of the matter under investigation. As interception of communications without the consent of the parties is a serious interference with privacy, such measure can be justified only if the offence under investigation is a serious in nature.

66. Subsection (1) (a) (iii) is essential to tackle the issue of mutual legal assistance in investigating serious crimes. This provision is essential as new means of communications may entail transborder transmissions of data. This makes international cooperation important. The country shall be able to respond to requests for mutual legal assistance requiring the interception of communications.

67. The provision of subsection (1) (b) is essential to ensure that the interception is authorised only with regard to the investigation of particular case. It is necessary to provide that a judge (magistrate) may authorise interception only with regard to specific crimes, national security issues or requests for mutual legal assistance and then only if the interception will support the investigation. There must be a ground for suspicion and interception must not be authorised on the off-chance of discovering crime.

68. The issuance of an interception order is further restricted by virtue of subsection (1) (c) to the cases where other procedures for obtaining information have not been or are unlikely to be successful or are too dangerous to apply in the circumstances or are impracticable due to the urgency of the case. This provision is needed to ensure that interception is not authorised unless the information is not reasonably available by less intrusive methods. The authorisation shall be justified not on the ground of relative ease of deploying interception techniques, but the reasonableness of carrying it out. This justification balances efficiency with the competing public interest in providing protection for the privacy of communications. It ensures that the means of investigation are proportionate to the immediacy and gravity of the crime.

69. Subsection (1) (d) provides that an interception order shall be issued only if it can serve in the best interests of the administration of justice. It obliges the judge (magistrate) to take these interests into account in granting authorisation. This is an additional safeguard to impose more stringent controls if the law enforcement agency merely wants to gather intelligence.

70. As an additional safeguard that ensures that each application is decided on the individual basis, subsection (2) enables judge (magistrate) to require additional information related to the application.

Section 8. Scope and Form for Interception Order

71. Section 8 provides rules on the scope and form of the interception order. To secure that the interference with privacy is kept to a minimum, it is necessary to establish the formal requirement of authorisation and to permit it only to be conducted by particular persons and only for certain address/person/communication. A set of requirements with regard to scope and form of the interception order aims to provide the certain formal framework for each case of interception, restrict the power to intercept and decrease the impact of the interception to third parties.

72. As no interception can take place without and interception order, the order must be specific as to what the person executing the interception can do. Furthermore, to safeguard the privacy, the judge (magistrate) should have the power to impose conditions that he may consider appropriate.

73. According to Subsection (1), an interception order shall be issued in the prescribed (written) form. The written form is essential to balance two important components: firstly, to secure the right to intercept and to request assistance, and, secondly, to restrict this right to particular person/address/communications. Thus, the written form of the interception order countervails the necessity to effect the particular intrusion with the need to eliminate the prospect for abuse. It is very important for an interception order to be as specific as possible. Subsections (1) (a), (b), (c), and (d) provide the scope of the authorisation with regard to the authority of the person executing it.

74. Subsection (2) serves as a measure balancing the authority granted by virtue of subsection (1). In order to strictly limit the authorisation to only a certain person and prevent any kind of abuse, Subsection (2) requires that either the person or the set of premises to be intercepted is named or described by the order. To comply with this provision, the interception order shall identify communications that should be intercepted either to or from one particular individual specified in the interception order or one particular address specified in the interception order. This is necessary to ensure that interception can only be permitted for the investigation of particular crime and not as a general monitoring measure.

79. There was a discussion in the Working Group with regard to the identification of the set of premises or communication devices from/to which communication is transmitted. The Working Group agreed that the term 'address' should be used in order to identify a particular set of premises, or phone number, or e-mail address for the interception. Following this discussion, the Working Group agreed that the definition of 'address' should be defined as follows: Section 9 "address" includes premises, email address, telephone number, or any number or designation used for the purpose of identifying communications networks, providers or apparatus.

80. Subsection (3) provides the possibility to include an entry clause in the interception order. The execution of the interception order may require entry to private premises. In the absence of a power to enter premises, an authorised officer would have to apply for a separate order under existing national legislation authorising him to enter the target premises. However, since interception can be granted only for investigation of serious crimes; the separate application is undesirable since it may cause delays in execution of the interception order.

81. To protect the privacy rights, the clause authorising entry to premises shall be made only for the purpose of the interception but not otherwise. The provision of subsection (3) allows authorization of entry to any premises specified in the order for the purpose of installing, maintaining, using or recovering any equipment used to intercept communications specified in the order. To secure that the prospective for abuse is eliminated, this subsection requires that any premises should be exactly specified in the entry clause and an authorised officer may enter them only for the particular purpose.

82. Subsection (4) requires the identification of an authorised officer on whose behalf the application is made; the person who will execute the interception order and the communications provider to whom the interception order should be addressed. This provision is an important a safeguard to limit the number of persons enabled to execute interception. Furthermore, it meets the general principle to keep orders as specific as possible to prevent the opportunity for abuse.

83. In addition, the interception order that contains the entry provision shall specify the permitted time of the entry and any additional measures to be taken in order to carry out the measure.

84. Since the interception order is issued only on the basis of particular grounds, which are individual for each case, the judge (magistrate) shall be vested with the power to impose additional conditions that will reflect the nature of the particular case. Subsections (5) and (6) are implemented to enable the judge (magistrate) to define ancillary provisions, conditions or restrictions relating to the interception of communications authorised in the order.

Section 9. Duration and Renewal of Interception Order

85. Section 9 is related to the duration and renewal of an interception order. The principal aim of this Section is to limit the authorisation to intercept to a certain period of time to avoid endless interception.

86. Furthermore, this Section provides a regulation for the renewal of the interception order when the period of validity established by this model Act and/or specified in the interception order turns out to be too short to reach the aim of the interception. The latest option is critical if it is necessary to continue the interception without interruption caused by a new application.

87. The limitation of the duration of the interception order to a certain (relatively short) period of time is a common approach in the majority of jurisdictions. However, the defined time period varies significantly - e.g.: 3 or 6 months (Australia), 6 months (OECS Model Law), 3 months (Hong Kong).

88. The necessary duration of the interception was intensively discussed and different aspects were considered. On the one hand, it is necessary to reflect that interception is a severe measure that should not be used unless it is absolutely essential. Thus, the duration of the order shall be limited. Furthermore, the longer the duration of an order is, the more likely it is that personal information, which is not relevant for an investigation, will be intercepted. This factor shall be taken into account when establishing the period of validity.

89. On the other hand, investigation of serious crimes may take time. If the maximum duration is too short, it could lead to a large number of applications for renewal and block resources.

90. Subsection (1) provides that the period of validity of an interception order shall not exceed 90 days. The suggested duration – 90 days – is an average period extracted from national approaches. The country may decide to change the duration within the implementation. The period of validity shall be specified by a judge (magistrate). This subsection also deals with the application for the renewal of an existing order.

91. Since authorisation of interception is subject to an *ex parte* application process, it is necessary to provide the same safeguards for the renewal of the interception order that are implemented with regard to the initial applications. Therefore, the form and the contents of application shall be the same. A renewal of the order may be granted by a judge (magistrate) based on an application made by the Director of Public Prosecutions on behalf of an authorised officer at any time before the order (or any current renewal of the order) has expired.

92. The Working Group discussed whether the application for the renewal should go through the same procedure and has to be in the same form as the initial application. The Working Group decided that the procedure for renewal should be as close to the procedures for the initial application as to keep all safeguards and prevent the risk of abuse of the power to intercept. Application for the renewal shall justify the circumstances for the renewal, give the reasons for the period for renewal and specify what has been done in order to carry out the existing order. That is why subsections (3) and (4) establish the same requirements for the application for the renewal that are established for initial applications. Furthermore, to provide the full particulars of the case, the application shall contain information on the execution of the current interception order. This is necessary to ensure that the interception is reasonable and focuses on investigating a particular crime. To enable the smooth examination of each application for renewal, Subsection (5) vests the judge (magistrate) with the ability to require additional information for processing the application.

93. Subsection (6) provides a safeguard related to the grounds for an interception: a judge (magistrate) may only renew an interception order if he or she is satisfied that the circumstances, which have been a ground for the authorisation to intercept still apply.

94. According to Subsection (7) the duration of every renewal of an interception order may not exceed the general period of validity (as suggested by the legislative text, 90 days) and shall be specified by a judge (magistrate) in the renewal.

95. Since interception represents a serious intrusion of privacy, it is very important to assure that it will be terminated as soon as there is no necessity to intercept anymore. To guarantee this principle, Subsection (8) requires an authorised officer to whom the order is issued or a person acting on his or her behalf to apply for the revocation of the interception order if it appears that an interception order is no longer necessary.

Section 10: Modification of Interception Order

96. Section 10 enables an authorised officer to apply for modification of an existing interception order if the circumstances have changed. This can be applicable in cases where the address of the premises of the suspect, phone numbers, or any other identification criteria specified in the interception order, changes. The process of application remains the same to secure that all safeguards are applicable. An application for modification of the existing interception order should be made by Director of Public Prosecutions on behalf of an authorised officer or by an authorised officer, depending on the approach taken. The grounds for the execution of the interception shall remain the same.

Section 11: Revocation of the Interception Order

97. This section is implemented to ensure that the interception order will be revoked when there is any abuse of the right to intercept or if interception is not necessary anymore. This is an essential mechanism to guarantee that the interception is in full compliance with the requirements of the Act. In addition, it should ensure that the interference is used only as an exceptional measure. The Section provides the grounds and procedure for revocation of the authorisation for interception. The Working Group changed the suggested term 'termination' to the term 'revocation'.

99. According to Subsection (1), an interception order may be revoked by a judge (magistrate) if an authorized officer fails to submit a report on progress in accordance with Section 15; or if the judge (magistrate) upon receipt of such report on progress is satisfied that the objectives of the interception order have been achieved; or the grounds on which the interception order was issued expired; or the conditions of the initial application have changed in a way that an application would not be possible anymore.

100. To establish the formal requirements related to the revocation and to ensure that an authorized officer is notified forthwith about the revocation, Subsection (2) defines that the notification of revocation of the order should be forwarded in written form to the authorised officer.

101. The aim of the Subsection (3) is to guarantee that if an interception order is revoked, the execution stops immediately. It requires an authorised officer to remove any intercepted device that was installed to carry out the interception. The de-installation needs to take place as soon as possible after receiving the information about the revocation.

Section 12. Consequences of Revocation

102. This section provides a safeguard for the case of revocation of the interception order. Since the interception order is revoked if the requirements for an interception established by the legislative text are not met anymore, it is necessary to ensure that the intercepted data are not used in criminal proceedings. Section 12 declares evidence that was collected while a order was revoked inadmissible unless the court decides that the admission of such evidence would not render the trial unfair.

Section 13. Urgent Application

103. Section 13 is essential for urgent cases that require an interception to be carried out as soon as possible as delays would impair the investigation. It provides the ground and procedure for such urgent applications.

104. In those cases oral applications are permitted. It is highly unlikely that an authorised officer would in urgent cases have the time to draft and submit a written application to the court. The Working Group therefore decided that there should be an emergency mechanism that enables an authorised officer to obtain an order under such circumstances.

105. Almost all national approaches do in certain cases permit urgent authorisation of interception. The procedures have been drafted in accordance with the OECS Model Law and New Zealand legislation.

106. According to Subsection (1) a judge (magistrate) may in urgent situations dispense with the requirements of a written application and allow the Director of Public Prosecutions on behalf of an authorised officer to orally apply for an interception order. The judge (magistrate) shall issue the order if he or she is satisfied that circumstances exist that would justify the grant of an interception order under Section 8.

107. To ensure the formal procedure of the application, Subsection (2) establishes the requirements that any application for an emergency order should meet. Firstly, it should contain the information referred to in subsection (2) of Section 6 which is required for the application for an interception order; secondly, it should indicate the particulars of the urgency of the case or the other exceptional circumstances which, in the opinion of the authorised officer justifies an oral application. Oral application should also comply with any directives, which may be issued by the judge (magistrate).

108. According to Subsection (3) a judge (magistrate) issues an emergency interception order only if he or she is satisfied that there are reasonable grounds to believe that the interception order shall be issued and it is not reasonably practicable to apply in written form. This provision aims to ensure that the urgent order can be granted only in exceptional circumstances.

109. There was a discussion in the Working Group about the opportunity to apply the rules of urgent application to the procedure of the renewal of the existing interception order. The major concern was how the appropriate checks and balances afforded by the clauses on the urgent application would apply in this case. The Working Group agreed not to allow oral application for standard cases of renewal.

110. To ensure that the records are kept for every emergency order, Subsection (4) requires a judge (magistrate) to keep a written note about the particulars of the application if an emergency order is issued.

111. Subsection (5) provides that an interception order issued on the basis of an oral application should have the same scope as for standard interception orders. This provision aims to avoid different standards with regard to urgent applications and normal procedures. The Working Group discussed whether the urgent order should be issued in writing or orally. It was agreed that the interception order issued upon oral application should be in written form required by Section 9.

112. The period of validity for every emergency interception order is provided by Subsection (6) and should be 48 hours from the time it was issued. After the period the order shall expire. According to Subsection (7) a written application and affidavit should be submitted in accordance with the provisions of Section 6 within 48 hours. This provision aims to ensure that every application for an interception order is transparent and finally made in written form. In addition it aims to give a judge (magistrate) the opportunity to review the urgent decision if there is not enough evidence for granting the interception.

113. There was a discussion within the Working Group about the procedure (written application) following the issuance of urgent interception orders. Some Consultation Workshop participants had concerns regarding the necessity to do paperwork in a short period of time. However, the Working Group agreed that it is necessary to require a written application to eliminate the prospect for abuse.

Since 48 hours is only a recommended duration of the urgent orders, the country may choose to provide a longer period of validity for urgently issued orders.

114. Subsection (8) establishes the procedure of reviewing the decision to grant an urgent order. This procedure is necessary to ensure that the derogation from formal procedure of application is justified or, if not, the order is revoked.

Section 14: Report on Progress

115. Report on progress is a necessary measure in oversight of the execution of interception orders. It enables a judge (magistrate) who has issued the order to be sure that interception is carried out in accordance with law and legal authorisation. This approach is for example used in the OECS Model Law on Interception of Communications. Section 14 gives a judge (magistrate), who has issued an interception order, the power to order the authorised officer on whose behalf the relevant application was made, to report in writing about the progress that has been made or any other matter that the judge (magistrate) considers necessary. Such order is binding and may entail the revocation of the interception order as defined by Section 11. The request under Section 14 can be made by a judge (magistrate) at the time of issuance of the interception order, or at any stage before the date of expiry.

116. The requirement for the Report on Progress also aims to balance administrative and judicial systems of controls.

Section 15: Final Report

117. This section is an option which may implement as an additional safeguard. The requirement of a final report about the results of the interception is implemented in some countries such as Australia and New Zealand. It requires an authorised officer to submit a final report on details of the interception including the results that were obtained. In this regard, the final report also serves as an additional instrument to secure compliance with the rules about confidentiality of intercepted communications as provided by Section 22.

118. Subsection (2) establishes a set of requirements related to form and content of the final report. It should be noted that special attention is paid to destruction of irrelevant information as a safeguard.

119. However, it is recognized that the country may experience difficulties in implementing this provision as the obligation goes along with additional paperwork and possible privacy concerns. The country therefore has the option of excluding this requirement.

PART III – EXECUTION OF INTERCEPTION

120. Part III establishes the duties and responsibilities of public bodies (authorised officer) and persons to execute interception. This section provides an essential framework for the process of carrying out the interception. It includes regulations related to the obligation to provide assistance. It also contains provisions dealing with the confidentiality of the intercepted information and obligation to destroy interception records. Strict regulations and safeguards are provided to ensure that information is kept confidential and irrelevant data are destroyed.

Section 16: Execution of Interception Order

121. This section is aimed at enabling an authorised officer to intercept communications specified in the order and in accordance with its terms. In addition, it grants an authorised officer the power to require a person that is specified in the order to intercept communications or to assist in the execution of interception. This duty to provide assistance is crucial since law enforcement agencies very often

depend upon the support from the person who has specific knowledge about communications networks or operates them. However, the obligation to provide assistance is limited to the scope of authorisation and duties specified in the interception order. This provision is essential to ensure that no unreasonable demands are made with regard to the person that is required to provide assistance. It provides the right to refuse a request for assistance which is not in compliance with the interception order.

122. Subsection (3) is necessary because the interception often interferes with the privacy not only of the person whose communications are subject of the interception. The third parties' right to private communications is often affected by the interception order as well. In order to limit the intrusion into third parties' lawful interests, this subsection obliges an authorised officer or a person who intercepts or assists in the interception of communications to take all reasonable steps to minimise the impact of interception on third parties.

123. The Working Group decided to add an additional provision to Section 16: Subsection (4) provides that no criminal or civil liability shall incur from the acts of an authorised officer or person if they are acting in compliance with an interception order. The same applies to anybody, who aids in good faith a person who he or she believes on reasonable grounds is acting in accordance with authorisation for interception. This provision is introduced to protect the person lawfully executing interception.

Section 17: Entry on Premises for the Execution of Interception Order

124. Section 17 provides the framework for the execution of the entry clause in the interception order, if there is one. The application of an interception order which contains a provision enabling the authorised officer to entry on premises shall be made in compliance with the Section 17 that permit an authorised officer to enter the premises at any time specified in the interception order and perform any act related to the purpose of the interception order.

Section 18: Duty to Provide Assistance

125. This section provides coercive measures to facilitate the interception of communications. It obliges a person, who provides communications services, to permit, and assist, if reasonably required, an authorised officer to exercise an interception order. To prevent the abuse of the power to request assistance, Subsection (2) provides that the duty of a person to intercept shall be specified by a judge (magistrate) in the interception order. This provision is essential to eliminate the prospects for abuse, especially because Section 19 creates an offence on the failure to assist.

Section 19: Failure to Assist

126. Pursuant to Section 19, any person who is required to provide assistance to an authorised officer by virtue of an interception order and refuses to do so commits an offence. The criminalization of the refusal to provide assistance is necessary because the interception order is granted in exceptional circumstances for the investigation of serious crimes and the success in executing the order often depends on the assistance from communications operators. When the request for assistance is refused, it may undermine the investigation and hamper the administration of justice in general.

Section 20: Confidentiality of Intercepted Communications

127. The privacy concerns and the need to maintain the secrecy of interception justify the requirement for confidentiality and for an obligation to destroy irrelevant data. There is also the need to protect to the feasible maximum the privacy of third parties whose communications are intercepted without their consent. To address this need for confidentiality, laws in many countries, such as in Australia, Canada, New Zealand, and South Africa all contain provisions prohibiting unauthorized use or disclosure of intercepted material.

128. Following this approach, Subsection (1) of Section 20 places strict safeguards on the extent to which intercepted material may be disclosed, copied and retained, requiring each of these to be kept to a minimum and obliging an authorised officer to make a set of arrangement necessary to ensure the confidentiality of interception. Providing robust safeguards for the process of execution of interception order with regard to the confidentiality of information, Subsection (2) specifies particular information on interception of communications and execution of interception order that should be kept confidential.

Section 21: Failure to Keep Information on Interception Confidential

129. Section 21 gives further protection of confidentiality of intercepted communications by establishing an offence for intentionally and without lawful excuse or justification disclosing anything that he or she is required to keep confidential under the provisions of Section 20.

Section 22: Destruction of Records

130. The provision is regulating the deletion of records. It is essential because not all data gleaned from an interception is relevant. Since interception of communications normally lasts for weeks or even months, it is very likely that personal information not relevant for the investigation may be obtained. Much of the information gained as a result of interception relates to third parties who have contacts with those targeted by the interception. The possibility of keeping this data will certainly result in an invasion of privacy both of third parties and of the target of interception. From a privacy point of view, the person whose rights have been affected by an interception ought to be notified about the infringement. This entails the problem of subject, time and circumstances of such notification. All these problems could be avoided if the privacy of the person affected by an interception could be safeguarded by the destruction of the intercepted material.

131. In order to protect privacy, Section 22 contains an obligation to immediately destroy any records that are not related to the objectives of the interception order. In addition, Subsection (2) requires the destruction of any records as soon as it appears that no proceedings or no further proceedings, will be undertaken in which the information would be likely to be required as evidence. Subsection (2) should apply with the exclusions established by Subsection (3) which states that the destruction obligation shall not apply to any record of any information adduced in proceedings in any court.

132. In order to control the requirement of keeping intercepted communications confidential and to destroy irrelevant information, Subsection (4) obliges an authorised person to provide the information in compliance with Subsection (2) to a judge (magistrate) in the final report on the execution of interception order. This provision is only relevant if the country includes the obligation related to a final report.

Section 23: Failure to Destroy Records

133. This section criminalises the failure to comply with the requirements to destroy records. The aim of this provision is to implement another strong safeguard to protect the privacy of communications and to ensure that all information irrelevant to the purposes of the interception is destroyed.

PART IV – INTERCEPTION EQUIPMENT

134. It is essential to regulate interception equipment, since the use of electronic devices to intercept communications constitutes the *prima facie* threat to the right for private communications. The necessity to prohibit the use of equipment with interception capabilities was widely agreed within the working group. However, there is no exact answer which mechanism for prohibition on and monitoring of the use of interception equipment is most effective. Two possible options were discussed by the Working Group. The first option was to prohibit the possessing, selling and acquiring of any device primarily designed to intercept communications and establish a limited number of exemptions for the

law enforcement agencies, government and communications operators. However, this approach raises the problem of 'dual-use' devices without solving it. Furthermore, during the discussion it was noted that the scope of such prohibition is uncertain.

135. The second approach is to list the equipment with interception capabilities to specify the extent of the restriction. This approach follows the model of South Africa and the OECS Model Law on Interception of Communications. Yet the main argument against this framework was the practical implementation of this provision and the feasibility of creating and maintaining the list.

136. While the Working Group agreed to the limitation of trade and the use of interception equipment, there was an intensive debate about the appropriate approach regarding the implementation. The Working Group discussed two abovementioned options, but no consensus was reached on this issue. Thus, the provisions of Part IV should be considered as a recommendation for should the country decide to follow the approach and create and maintain a list of equipment with the interception capabilities.

137. The Act uses the list-based approach. The aim of this approach is to prohibit certain acts and to establish control on unlawful manufacture and possession of interception equipment. In addition, it seeks to regulate the process of authorisation for such equipment. It also aims to protect all interested parties by requiring a consultation process before the use of particular equipment is restricted or prohibited.

Section 24: Listed Equipment with Interception Capabilities

138. To secure the approach to list the equipment with interception capabilities, Section 24 defines that the Minister may by notice publish in the Gazette declare any electronic, electro-magnetic, acoustic, mechanical or other equipment or device, that is primarily useful for purposes of the interception of communications, under the circumstances specified in the notice, to be listed equipment. The process of issuing such a notice is established by Subsections (2) – (7). Section (4) provides a safeguard for all interested parties obliging the ministry to invite them to submit written comments with regard to the proposal. This provision guarantees the transparency of the procedure and the participation of all interested parties. It also aims to protect the development of technology.

Section 25: Prohibition on Manufacture, Possession and the Use of the Listed Equipment with Interception Capabilities

Section 26: Authorisation to Use the Listed Equipment with Interception Capabilities

139. To define restriction with regard to equipment contained in the list, Section 25 prohibits the manufacture, possession and use of listed equipment with interception capabilities unless authorised. The authorisation may be given under the Section 26 which provides a ministry with the power to grant an exemption if it is in the public interest or the purpose for which the listed equipment will be manufactured, assembled, possessed, sold, purchased or advertised is reasonably necessary or if there are special circumstances which justify such exemption. Section 26 also establishes the requirements for the form and duration of certificate of exemption.

Section 27: Offence

140. In order to restrict the manufacture and possession of equipment with interception capabilities, Section 27 criminalises certain acts related to listed devices.

PART V – DISCLOSURE OF STORED COMMUNICATIONS DATA

141. Part V was developed to provide the country with the possibility of disclosing stored communication data which have already passed transmission and are therefore by definition not considered as a subject for interception.

142. This part was constructed in the manner protecting the privacy of stored communications data. It was included as in a number of cases it can be necessary to obtain stored information such as location data when communications cannot be intercepted because they have already passed the process of transmission. The Working Group, therefore, agreed that not including this instrument in the model legislative text could force countries to introduce this necessary instrument in a second approach. The OECS Model Law on Interception of Communications as well legislation in Australia and the United Kingdom follow the same approach and combine interception legislation with legislation related to the disclosure of stored communications data.

143. There was an intensive discussion in the Working Group about this topic. While the opinion was raised that these provisions have been helpful to law enforcement in some jurisdictions, it was widely agreed that they were outside of the scope of the model legislative text. As such, the country has the option of implementing or not implementing it.

144. Thus, the following provisions are optional and represent recommendations which the country may decide to follow.

145. Part V of the model legislative text prohibits the access to stored communications data and establishes a limited set of conditions under which a disclosure order can be issued. The nature of access to stored communications data is different from the interception of communications. Access to the stored communications does not represent a collection of data during their transmission and does not require interception equipment to be installed. That is why less strict rules are applied in the case when access to stored data is needed. However, stored data are protected by virtue of the law as communications during their transmission. Unlawful access to stored communication data is prohibited by Section 28.

Section 28: Prohibition on Access to Stored Communication

146. Similarly to the criminalisation of unlawful interception, this Section criminalises unlawful access to stored communications data and explains the circumstances under which such access can be considered lawful. The Working Group decided to include the criminalisation to ensure a strong protection of the privacy and protection from unlawful intrusion.

Section 29: Disclosure of Stored Communications Data

147. Section 29 enables the designated person to require a communications provider to obtain and / or disclose stored communications data by using a disclosure order. As a safeguard to protect confidentiality of stored communications data, Subsections (2) and (3) limit the conditions under which disclosure orders can be issued to:

- interests of national security;
- purpose of preventing or detecting crime or of preventing public disorder;
- interests of public safety;
- purpose of protecting public health;
- 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;

and prohibit the issue of a disclosure order unless the designated person is satisfied that it is necessary to obtain the data and disclose its data to an authorised officer.

148. Subsection (4) provides a set of requirements with regard to the disclosure order. It requires that the circumstances and reason for granting it shall be specified as well as the communication data in relation to which it applies and the manner in which disclosure is to be made. In addition, the authorised officer needs to be identified. The reason for establishing the requirements with regard to the disclosure order is to make the procedure transparent and to limit the disclosure to the individual case by specifying all particulars of the authorisation.

149. Subsection (5) establishes a set of restriction to the authorisation that can be made by prohibiting any requirement related to communications data to be obtained after the end of the period of one month beginning on the date on which the order is issued. It also forbids the disclosure of any communications data not in the possession of the provider of the communications service, or required to be obtained by him or her, after the end of such period.

150. In order to keep disclosure order confidential, Subsection (6), subject to limited exclusions provided by Subsection (7), requires a communication provider, who receives such order to keep existence and operation of the order as well as related information confidential. To ensure the right of the communication provider to seek legal advice, Subsection (7), among other exemptions, enables communication operator to disclose information to attorney-at-law within legal consultation.

Section 30. Failure to Keep Information on the Disclosure Order Confidential

151. In order to protect the secrecy of the disclosure order, Section 30 criminalises the failure to meet confidentially requirements.

PART VI – COSTS OF INTERCEPTION

152. The allocation of cost was one essential point of discussion in the Working Group in the context of execution of interception. It is especially relevant with regard to the implementation of the duty of providers to provide assistance. Law enforcement agencies very often have to rely on the support from communication providers while executing interception.

Section 31: Allocation of Costs

153. This section provides that any costs generated by the development of technical capacities to intercept communication on the provider level (including the investment, technical, maintenance and operating costs) must be borne by that communications provider. However, the country may establish the model of reimbursement of direct costs incurred by communications providers in respect of personnel and administration required for the purposes of providing assistance in the execution of interception orders.

154. There was a debate within the Working Group and the Consultation Workshop plenary participants about the suggested approach. The debate focused on the vagaries of public policy and the impact that such position could have on the cost burden. In this respect, the debate took account that operators already have to cover the cost of other services. It was noted that such a position would be based on the fiscal position of individual states and could have an impact on the attractiveness of a jurisdiction to ICT investment. As a consequence of the controversial debate the Working Group decided to leave the decision about costs to the member states.

PART VII – SAFEGUARDS

Section 32. Professional Secrecy

155. This section refers to certain types of professional communications that are subject to the obligation of professional secrecy under national laws or regulations. The provisions safeguarding professional secrecy shall be strictly limited to those types of privileged communications that are protected by existing national laws, such as communications between attorney-at-law and a client, medical practitioner and a patient, communications protected under the law regulating financial and banking secrecy. The Act itself does not establish the privilege for communications in general.

156. The protection of professional secrecy does not mean that communications of the particular person cannot be a subject of interception at all. For example, if an attorney-at-law is suspected of a crime that allows interception, the authorisation for interception shall be granted. However, the data gathered by such interception shall not be presented as evidence in court and shall remain privileged, if they contain professional secrecy.

157. If the country decides to follow the approach under Section 33 and implement such safeguards, the list of professional secrecy protected by virtue of law shall be constructed in accordance with existing legislation.

Section 33: Monitoring of Communications Interception

158. Section 33 provides for the creation of an independent monitoring authority. Independent monitoring of interception is necessary to strengthen the system of checks and balances with regard to such an intrusive measure as interception.

159. As an option, the country may vest any authority that is not actively involved in the investigation process, and has the capacity to perform the necessary functions to supervise the interception, with the functions of the independent monitoring authority. This option is especially relevant if there is a lack of resources.

160. This Section also makes recommendations with regard to the functions of an independent monitoring authority, which may be specified if the country so chooses.

161. The country may decide to implement this section depending on the availability of resources.

Section 34: Independent Commissioner on Interception of Communications

162. This section provides recommendations with regard to the creation of an independent oversight body (Independent Commissioner on Interception of Communication). This Section may be implemented only if considered necessary.

PART VIII – ADMISSIBILITY OF EVIDENCE

163. The question was discussed whether the model legislative text should cover the issue of admissibility of intercepted data as evidence if it is not covered by other legislation.

164. The Working Group decided to leave an option to include regulation of the admissibility of evidence. However, it was agreed that each jurisdiction shall develop such provisions in compliance with national legislation. Therefore, the only recommendation that could be made was to ensure that either (1) national legislation covers the issue of the admissibility of evidence obtained as a result of interception; or (2) provisions are developed in compliance with the national approach to the admissibility of evidence to cover this issue in the law regulating interception.

PART IX – SCHEDULE

165. The Schedule represents a list of serious offences that, subject to Section 7, can justify the interception as a measure to carry out an investigation.

166. The Act allows the relevant minister to add or delete offences from the list contained in the Schedule, as required.

167. The Act also enables the minister to make regulations to give effect to the purposes of the Act.

168. The Schedule provides the following list of recommended offences:

- Murder or Manslaughter or treason.
- Kidnapping or abduction.
- Money laundering contrary to the [Proceeds of Crime and Money Laundering (Prevention) Act.
- Producing, manufacturing, supplying or otherwise dealing in any dangerous drug in contravention of the Dangerous Drugs Act.
- Importing or exporting a dangerous drug in contravention of the Dangerous Drugs Act.
- Importation, exportation or trans-shipment of any firearm or ammunition in contravention of the Firearms Act.
- Manufacture of, or dealing, in firearms or ammunition in contravention of the Firearms Act.
- Illegal possession of a prohibited weapon or any other firearm or ammunition contrary to section X of the Firearms Act.
- An offence contrary to section X of the Prevention of Corruption Act.
- Arson.
- International Convention on hijacking, terrorist offences, etc.
- Prevention of Terrorism Act.
- Attempting or conspiring to commit, or aiding, abetting, counselling or procuring the commission of, an offence falling within any of the preceding paragraphs.

Annex 2

Report on Proposed Policy on Interception of Communications

Grenada

Introduction

1.1 Why an Interception of Communication Policy?

The Government of Grenada, like many of its fellow Organisation of Eastern Caribbean States (OECS), territories and other countries worldwide has recognized the social and economic benefits to be derived from Information Communications Technology, (ICT). Properly engaged, ICT is a significant tool in the fight against poverty, as well as in the enabling of sustainable development.

The Government's mission as reflected in its Mission Statement in the 2006-2010 ICT Strategy and Action Plan, "*To put Information and Communication Technologies (ICT) at the center of Grenada's social and economic development as a dynamic industry sector in itself, and in support of the development of other sectors of the economy; To establish a Knowledge-based society as the platform on which to foster, accelerate and sustain long-term social, cultural and economic development*",[14] aptly reflects The Geneva Declaration of Principles of the World Summit on the Information Society (WSIS) which notes that "*…under favourable conditions, these technologies can be a powerful instrument, increasing productivity, generating economic growth, job creation and employability and improving the quality of life of all…"*[15]

The Government has declared its five (5) areas of priority as education, health and wellness services, tourism and hospitality services, energy development and agribusiness and ICT services, with ICT being both an enabling sector and a sector in itself.

ICT will undoubtedly enhance Grenada's competitiveness both regionally and globally, creating an environment supportive of new products and services, and requiring new skills and technologies. Without the proper legislative framework in place, it can also become a haven for criminals to expedite traditional crimes such as, trafficking in illegal drugs, trafficking in illegal firearms and ammunition, money laundering and human trafficking etc., using ICT.

The Government is however, cognizant of these challenges and the need to ensure the security of the ICT environment, which will aid in promoting the confidence of consumers and investors in utilizing ICT in Grenada, thereby enabling the development of an information society and economy.

As such it has recognized the important role which lawful interception of communications can play in combating cybercrime. This notwithstanding, it is also aware of the potential for controversy and abuse which may result if it is not properly regulated.

Thus in order to strike that balance between protection of citizens constitutional rights and promoting the confidence of consumers and investors in the use of ICT on the one hand, and facilitating the identification of perpetrators, the investigation and prosecution of cybercrime on the other hand, the government has recognized the need for policy to guide the development of effective legislation on interception of communications which makes it difficult to abuse the powers provided thereunder.

It is against this background that this policy to inform the proposed legislation governing interception of communications has been developed.

1.2 Policy on Interception of Communications

The Government of Grenada has both the responsibility and the power to formulate the relevant policy, to develop the requisite legislative and regulatory framework and to enact relevant and effective legislation/law to combat cybercrime in order to maximize the benefits which can be derived from an ICT-based economy and society.

[14] Page 12 of 2006-2010 Strategy and Action Plan
[15] International Telecommunication Union (ITU), WSIS Outcome Documents, December 2005, p.10

Mindful of the many challenges which come with the development of this type of society and economy, such as the potential for increased and more sophisticated criminal activity, and increased difficulty in detecting, investigating and prosecuting resulting crimes, the Government has taken the initiative to develop a sufficiently comprehensive policy on interception of communications to guide the development of effective legislation on interception of communications, which would provide a much needed tool in the fight against cybercrime.

The Government which is also committed to promoting public confidence in the use of ICT's for conducting business of all types and at all levels (both public sector such as e-government and private sector), as well as promoting the confidence of both internal and external investors, has recognized the need for the development of a new ICT specific legislative framework and infrastructure.

As such it has engaged Stage 2 of the HIPCAR Project[16] to develop relevant policies and legislation in the areas of cybercrime, interception of communications and electronic evidence. These three areas are the foundation areas required for the building of a knowledge based society and economy.

1.3 Purpose of the Policy

This policy is intended to provide a guiding structure for the development and implementation of effective legislation to govern the interception of communications, an essential tool in the fight against cybercrime and other serious crimes. It takes account of the possibility of the infringement of citizens' constitutional rights and of the abuse of the powers granted under the proposed Bill, and as such provides a framework to ensure that the resulting legislation embodies sufficient safeguards to prevent these occurrences.

This document therefore, sets out the policy which guides the development of the proposed Bill on Interception of Communications. Both the Policy and the Bill are based on the Model Policy Guidelines and Legislative Text on Interception of Communications, developed under Stage 1 of the HIPCAR Project.

The main aim of the Bill, which facilitates both regional and international cooperation, is to introduce a legal framework for the lawful interception of Communications within very definite parameters while at the same time prohibiting the unlawful interception of communications. It is intended to apply to serious crimes such as drug trafficking and money laundering etc and only in circumstances where there is no other option for obtaining the type of evidence required, or other methods are to dangerous to employ.

Background

2.1 Existing Interception of Communication Policy

Grenada presently has no formal policy directly addressing the interception of communications, nor is there in place any effective legislative framework governing the interception of communications.

With its mission of transforming Grenada into a knowledge based society and economy, and recognizing the potential for the rapid growth of cybercrime in such a society and its effects on the economy, the Government recognizes that a formal policy on interception of communications is an essential tool in ensuring the creation of a relevant and effective legislative framework which assists in the effective investigation of cybercrime and the prosecution of perpetrators, thereby safeguarding the interests of the citizens and investors alike and ultimately promoting their confidence and trust in the use of ICT's in transacting all types of business. In this regard the Government supports the following policy objectives:

[16] HIPCAR "Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures."

- To guide the development of an effective, technology neutral interception of communications bill, which augments the proposed cybercrime bill, and complements an ICT-knowledge-based society and economy; and
- To promote and enhance the trust and confidence of consumers of online services, by ensuring the proposed interception of communications bill provides relevant safeguards against the potential risks for abuse, while enabling the effective investigation of cybercrime and the prosecution of cybercriminals.

The HIPCAR Model Policy Guidelines are in this respect essential to the establishment of an interception of communications policy for Grenada, which is consistent with international standards and best practices and facilitates the harmonization of resulting legislation, both regionally and internationally.

2.2 What is Interception of Communications?

The development and proliferation of ICT's have provided new media and platforms through and on which both old and new offences can be committed.

In accordance with ITU's Toolkit for Cybercrime Legislation[17], "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."[18]

Such a definition explains the broad scope of "interception" as well as of the "communication" subject to it, which includes "content" (information communicated) and "traffic"(data relating to communication)[19]. It also outlines different means of communication which may be intercepted. Naturally, Internet-based communication – and especially cybercrime – constitutes an important portion of interception activities from the quantitative and complexity standpoints.

2.3 The Nature of Interception

Interception of communications is a very intrusive measure which impacts the individual's rights to privacy and also affects data protection. It is also often a point of controversy in many Caribbean States.

Therefore, in light of this and given the significant role it can play in helping to combat cybercrime, it requires sound policy initiatives to guide the development of legislation defining the parameters within which interception of communications can be lawfully executed, while at the same time legislating against unlawful interception.

This policy and the resulting proposed Interception of Communications Bill provide an effective framework within which to execute lawful interception of communications in Grenada.

---

[17] 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.

[18] Section 1 – Definitions, item "k".

[19] 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."

2.4 Legislative Approach

The proposed Bill, which is drafted using technology neutral language, also utilizes a 'light-touch' approach. Essentially, the Bill avoids over-legislating and facilitates both technological advancements and new and innovative developments in cybercrime.

The proposed Bill introduces a legal framework for the lawful interception of Communications within very definite parameters and at the same time prohibits unlawful interception of communication. It is intended to apply to serious crimes such as drug trafficking and money laundering, etc.

In light of the Government's mission and vision as stated in the 2006-2010 Strategy and Action Plan, the proposed Policy and Bill on Interception of Communications are necessary elements in creating a secure ICT-based environment in which to transact all types of business, as they provide the requisite infrastructure to aid in the fight against cybercrime, thereby promoting the confidence of consumers and investors in the security of engaging in electronic commerce in Grenada.

2.5 Linkage to Other Legislation

This policy is intended to provide a framework for the development of interception of communications legislation which facilitates both regional and international trans-border cooperation.

Regionally and internationally countries are faced with serious challenges resulting from cybercrime activities. This has resulted in a number of international and regional organizations, such as the United Nations, the International Telecommunication Union, the Commonwealth and the Council of Europe contributing to the development of model policy and law to assist in combating cybercrime.

This policy and the resulting proposed Interception of Communications Bill draw upon and are influenced by these sources.

Both the policy and the bill will directly affect legislation and or legal practices relating to the Criminal Code, the Proceeds of Crime Act, the Telecommunications Act, the Computer Crimes and Cybercrime Act and the Evidence Act.

They will also have some impact on certain constitutional rights, and on laws pertaining to banking and to data protection.

Policy Objectives

3.1 Complementing the National Strategy and Action Plan

This policy aims to complement the 2006-2010 Strategy and Action Plan of Grenada, by aiding the building of the trust and confidence of the Grenada public, as well as investors, both internal and external, in conducting business and transacting online.

This is done by providing the guiding principles for the development of a relevant and effective interception of communications legislative framework.

The policy provides that legislation should allow the interception of communications in certain circumstances and in strict compliance with stipulated procedural requirements. It also requires effective procedural instruments enabling competent authorities to apply for, obtain and execute interception orders and enables transnational cooperation in investigations.

3.2 Objectives of the Proposed Policy on Interception of Communications

The objectives of the proposed Policy on Interception of Communications are as follows:

- To guide the development of an effective cybercrime bill, which complements an ICT knowledge-based society and economy; and
- To promote and enhance the trust and confidence of consumers of online services, by ensuring the resulting bill provides relevant provisions enabling the detection and effective investigation of cybercrime, the prosecution of cybercriminals and penalties commensurate with the effects of the crimes perpetrated on the victims.

In light of rapid technological advancements and the ever increasing sophistication of cybercriminals, as well as the recognition of the need for harmonized legislation which lends itself easily to regional and international trans-border cooperation, the Government is now embarking on the development of a cybercrime policy and cybercrime bill, which conforms to international standards and best practices and, which is a supporting pillar of the knowledge-based society and economy, into which Grenada is intended to be transformed.

Key Principles

The Government of Grenada is patently aware of the sophistication of today's criminals, who engage the use of fast pace technological advancements in the execution of crime. As such this policy promotes the development of technology neutral legislation which promotes the doctrine of cooperation and consequently enables law enforcement to become more effective in the fight against crime. Below are the guiding principles which inform the development of the Proposed Cybercrime Bill.

4.1 Establishment of Common Interpretations for Key Terms

Legislation on cybercrime should properly define terms such as "computer", "computer system", "device" and "hinder" etc., using sufficiently broad wording and where possible illustrative examples. It should clearly provide which terminology shall be left for judicial construction and the procedure for ensuring the alignment of both the judicial and statutory interpretations/definitions. As far as possible, technical terms should be defined, and harmonization should be facilitated through the sharing of judicial precedents. Training material should be developed, where necessary, to provide investigators, prosecutors, judges and the relevant stakeholders with the interpretation of said terms.

4.2 Development of Substantive Criminal Law

The legislation should contain provisions covering the most common and internationally accepted forms of cybercrime as well as those offences that are of specific interest for the region e.g., SPAM. It should be compatible with both international standards and best practices, in order to ensure cooperation with law enforcement agencies from countries within and without the region.

It should provide for the criminalization of the intentional and illegal accessing of a computer system as well as the illegal remaining in the said system. Where circumvention of protection measures occurred to facilitate the interception of the transmission, an increase in the severity of the penalty should be considered.

The intentional and illegal interception of non-public data transmission, (illegal interception), should be criminalized, without hindering the lawful interception by competent authorities. Where circumvention of protection measures occurred to facilitate the interception of the transmission, an increase in the severity of the penalty should also be considered.

The cybercrime legislation should provide for the criminalization of the intentional and illegal interference with computer data. It should ensure that the application of the procedural instrument necessary for investigations is not hindered in cases where the offender commits several offences and each only leads to limited damage.

The intentional and illegal interference with computer systems, (such as denial of service attacks), should be criminalized, and consideration be given to an increase in the severity of the penalty provided for, in cases where critical infrastructure is affected. The law should similarly provide for the criminalization of the intentional and illegal production, sale and related acts, of tools that are primarily designed to commit computer crimes, while ensuring that the legitimate use of such software tools are not criminalized.

The Legislation should provide for the criminalization of intentional and illegal computer-related fraud and should ensure its compatibility with existing legislation criminalizing fraud, in circumstances where offenders are communicating with victims via electronic communications. Intentional and illegal computer-related forgery should be criminalized, ensuring that the legislation covers acts such as the sending out of phishing emails. Consideration should be given to increasing the severity of the penalty in cases where numerous emails are sent out.

The intentional and illegal production and sale of child pornography; and related acts should be criminalized, taking into account international standards. Additionally, the legislation should cover the criminalization of the possession of child pornography and gaining access to child pornography websites. There should, however, be an exemption to enable law enforcement agencies to carry out investigations.

The legislation should provide for the criminalization of acts related to the sending out of SPAM if it affects the ability of users to utilize internet access and should reflect the challenges related to attribution. It should also criminalize the intentional and illegal acts of identity-related crime, taking into consideration the different phases of identity theft, (obtaining, transferring and using identity-related information).

4.3 Development of Effective but Balanced Procedural Instruments which enable Competent Authorities to Investigate Cybercrime

No procedural instrument should interfere with a suspect's internationally or regionally accepted fundamental rights.

The legislation should enable competent authorities to order the expedited preservation of computer data, as well as the partial disclosure of preserved computer data. It should also enable competent authorities to order the production of computer data. The legislation should enable competent authorities to use specific search and seizure instruments related to digital evidence and computer technology. It should regulate search and seizure proceedings in such a way to avoid the collection of evidence being questioned, as not having been certified and produced as material evidence of the data collected, and of the existing digital environment.

Competent authorities should be enabled to order the lawful collection of traffic data and the lawful interception of content data. They should also be enabled to utilize sophisticated investigation instruments such as key-loggers and remote forensic software, to collect passwords used by a suspect, or to identify the connection used by a suspect. The legislation should, however, limit the use of such sophisticated instruments to cases of serious crime.

4.4 Development of Instruments for Transnational Cooperation in Cybercrime Investigations

The framework for international cooperation should reflect international standards of cooperation as well as the specific needs of cybercrime investigations. It should include the creation of a designated 24/7 point of contact for requests and enable the use of expedited means of communication such as email and fax.

4.5 Development of a Framework Regulating the Responsibility of Internet Service Providers

In cases where liability exists, the framework should limit the criminal responsibility of Access Providers with regard to offences committed by users of their service, if the provider did not initiate the transmission, did not select the receiver and did not modify the information contained in the transmission. The criminal responsibility of the Caching Provider should likewise be limited, if liability exists, for the automatic, intermediate and temporary storage of information. Also for the Hosting Provider, if liability exists, this should be limited by the framework, in cases where the provider has no actual knowledge about the existence of illegal data or immediately removes them upon obtaining such knowledge.

Bibliography

Council of Europe, Convention on Cybercrime, Budapest, Hungary, 2011, URL: http://conventions.coe.int/Treaty/en/Treaties/html/185.htm

European Parliament and the Council of the European Union, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *Official Journal L 201 , 31/07/2002 P. 0037 – 0047*, URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

European Parliament and the Council of the European Union, Directive 2006/24/EC European Parliament and the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal of the European Union, L 105/54, 13.4.2006, URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

Government of Grenada, ICT Strategy and Action Plan 2006-2010

International Telecommunication Union (ITU), HIPCAR Interception of Communications Assessment Report, Geneva, Switzerland, 2012, URL: http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/info-society.html

International Telecommunication Union (ITU), HIPCAR Interception of Communications Model Policy Guidelines and Legislative Texts, Geneva, Switzerland, 2012, URL: http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/info-society.html

International Telecommunication Union (ITU), ITU's Toolkit for Cybercrime Legislation, Geneva, Switzerland, URL: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf

United Nations Public Administration Network (UNPAN), OECS Interception of Communications Bill, page 6, URL: http://unpan1.un.org/intradoc/groups/public/documents/TASF/UNPAN024635.pdf
Organisation of Eastern Caribbean States, Saint Lucia, URL: http://www.oecs.org/projects/egrip/what-is-the-egrip

Annex 3

Participants at First Stakeholder Consultation Workshop on Cybercrime, e-Evidence and Interception of Communications

Co-organized with the Government of Grenada and the ITU/EU-funded HIPCAR Project
National Stadium, St. George's, Grenada, 15-16 February 2012

ORGANIZATION	LAST NAME	FIRST NAME
	ROBERTS	Vincent
Afi Ventour & Co	VENTOUR-DE VEGA	Afi
Caribbean Knowledge and Learning Network (CKLN)	BAILEY	Juan
Corporate Affairs and Intellectual Property	HENRY	Annette
Customs Department	MARSHALL	Lindonna
Department of Public Prosecution	GREENIDGE	Crisan
DIGICEL	ALLEYNE	Nadia
Division of Cooperatives	SLINGER	Carolyn
Economic Partnership Agreement (EPA) Implementation Unit	GARRAWY	Nicole
FLOW	MCINTOSH	Brent
FLOW Grenada Ltd.	BURKE	Edmund
FLOW Grenada Ltd.	LAWTON	Opal
FLOW Grenada Ltd.	PURCELL	Gail
Grenada Broadcast	GRANT	George
Grenada Co-operative Credit Union League	MOSES	Aaron
Grenada Industrial Development Corporation	VICTOR	Kent
Grenada National EPA Implementation (EPA) Unit	JOHN	Desmond
Grenada Postal Corporation	SYLVESTER	Ruben
Inland Revenue Department	LEWIS	Nelson
LIME	LANGAIGNE	Glendon
LIME	NOEL	Cecil
LIME	PITT	James
LIME	STEELE	Angus
Media Workers Association of Grenada	TITUS	Rawle
Ministry of Education	NURSE	Eric
Ministry of Finance	BURKE	Nazim

Ministry of ICT	**SIMON**	**Loretta**
Ministry of Legal Affairs	**BAISDEN**	**Ayesha**
Ministry of the Environment	**CHARLTON**	**Henry**
Ministry of Works	**CLARKE**	**Dennis**
National Insurance Scheme	**NOEL**	**Dwane**
National Telecommunications Regulatory Commission (NTRC)	**FERGUSON**	**Ruggles**
National Telecommunications Regulatory Commission (NTRC)	**FERGUSON**	**Aldwyn**
Prime Minister's Office, St. Vincent and the Grenadines	**THOMSPON**	**Jerrol**
Procurement Unit	**VICTOR**	**Terrence**
Royal Grenada Police Force	**DICKSON**	**Simon**
Royal Grenada Police Force	**GREENIDGE**	**Teron**
Royal Grenada Police Force	**NOEL**	**Franchesca**

Annex 4

Participants at Second Stakeholder Consultation/Validation Workshop on Cybercrime, e-Evidence and Interception of Communications

Co-organized with the Government of Grenada and the ITU/EU-funded HIPCAR Project
Ministry of Legal Affairs, St. George's, Grenada, 27 March 2012

LAST NAME	FIRST NAME
BAISDEN	Ayesha
BAKER	Wynette
BAPTISTE	Maureen
BOWEN	Christine
FOSTER	Francis
GOODING-De SOUZA	Camille
LASHLEY-BYER	Nicola
MARRAST-VICTOR	Kinna
OLOWU	Adebayo

Annex 5

Participants at Second Stakeholder Consultation/Validation Workshop on Cybercrime, e-Evidence and Interception of Communications

Co-organized with the Government of Grenada and the ITU/EU-funded HIPCAR Project
National Stadium, St. George's, Grenada, 28 March 2012

ORGANIZATION	LAST NAME	FIRST NAME
Financial Intelligence Unit (FIU)	GREENIDGE	Teron
FLOW	MCINTOSH	Brent
Grenada National EPA Implementation Unit	JOHN	Desmond
	ROBERTS	Vincent
Inland Revenue Department	LEWIS	Nelson
LIME	LANGAIGNE	Glendon
LIME	NOEL	Cecil
Ministry of ICT	SIMON	Loretta
Ministry of Legal Affairs	BAISDEN	Ayesha
National Telecommunications Regulatory Commission	FERGUSON	Aldwyn
Procurement Unit	VICTOR	Terrence
Royal Grenada Police Force	NOEL	Francisca