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

Interception of Communications:

Model Policy Guidelines & Legislative Texts

HIPCAR

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

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

Interception of Communications:

Model Policy Guidelines & Legislative Texts

HIPCAR

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

Disclaimer

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

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

Please consider the environment before printing this report.

Foreword

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

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

The project 'Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures' (HIPCAR) has sought to address this potential impediment by bringing together and accompanying all 15 Caribbean countries in the Group of African, Caribbean and Pacific States (ACP) as they formulate and adopt harmonised ICT policies, legislation, and regulatory frameworks. Executed by the International Telecommunication Union (ITU), the project has been undertaken in close cooperation with the Caribbean Telecommunications Union (CTU), which is the chair of the HIPCAR Steering Committee. A global steering committee composed of the representatives of the ACP Secretariat and the Development and Cooperation - EuropeAid (DEVCO, European Commission) oversees the overall implementation of the project.

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

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

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

I take this opportunity to thank the European Commission and ACP Secretariat for their financial contribution. I also thank the Caribbean Community (CARICOM) Secretariat and the Caribbean Telecommunication Union (CTU) Secretariat for their contribution to this work. Without political will on the part of beneficiary countries, not much would have been achieved. For that, I express my profound thanks to all the ACP governments for their political will which has made this project a resounding success.

Brahima Sanou
BDT, Director

Acknowledgements

The present document represents an achievement of the regional activities carried out under the HIPCAR project "Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures", officially launched in Grenada in December 2008.

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

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

The HIPCAR Steering Committee – chaired by the Caribbean Telecommunications Union (CTU) – provided guidance and support to a team of consultants, including Mr. Gilberto Martíns de Almeida, Dr. Marco Gercke and Ms. Karen Stephen-Dalton. The draft document was then reviewed, discussed and adopted by broad consensus by participants at two consultation workshops for the HIPCAR Working Group on Information Society Issues, held in Saint Lucia on 8-12 March 2010 and in Barbados on 23-26 August 2010 (see Annexes). The explanatory notes to the model legislative text in this document were prepared by Dr. Gercke addressing, *inter alia*, the points raised at the second workshop.

ITU would like to especially thank the workshop delegates from the Caribbean ICT and telecommunications ministries, representatives from the ministries of justice and legal affairs and other public sector bodies, regulators, academia, civil society, operators, and regional organizations, for their hard work and commitment in producing the contents of this report. This broad base of public sector participation representing different sectors allowed the project to benefit from a cross-section of views and interests. The contributions from the Caribbean Community (CARICOM) Secretariat and the Caribbean Telecommunications Union (CTU) are also gratefully acknowledged.

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

The activities have been implemented by Ms Kerstin Ludwig, responsible for the coordination of activities in the Caribbean (HIPCAR Project Coordinator), and Mr Sandro Bazzanella, responsible for the management of the whole project covering sub-Saharan Africa, the Caribbean and the Pacific (ITU-EC-ACP Project Manager) with the overall support of Ms Nicole Darmanie, HIPCAR Project Assistant, and of Ms Silvia Villar, ITU-EC-ACP Project Assistant. The work was carried under the overall direction of Mr Cosmas Zavazava, Chief, Project Support and Knowledge Management (PKM) Department. The document has further benefited from comments of the ITU Telecommunication Development Bureau's (BDT) ICT Applications and Cybersecurity Division (CYB). Support was provided by Mr. Philip Cross, ITU Area Representative for the Caribbean. Pre-formatting was done by Mr. Pau Puig Gabarró. The team at ITU's Publication Composition Service was responsible for its publication.

Table of Contents

Page

Foreword ..... **iii**

Acknowledgements ..... **v**

Table of Contents ..... **vii**

Introduction **1**

1.1. HIPCAR Project – Aims and Beneficiaries 1

1.2. Project Steering Committee and Working Groups 1

1.3. Project Implementation and Content 2

1.4.Overview of the Six HIPCAR Model Policy Guidelines and Legislative Texts Dealing with Information Society Issues 2

1.5. This Report 6

1.6. The Importance of Effective Policies and Legislation on Interception of Communications 7

Section I: Model Policy Guidelines – Interception of Communications **11**

Section II: Model Legislative Text – Interception of Communications **15**

PART I – PRELIMINARY 17

PART II – INTERCEPTION OF COMMUNICATIONS 18

PART III – EXECUTION OF INTERCEPTION 26

PART IV – INTERCEPTION EQUIPMENT 28

PART V – DISCLOSURE OF STORED COMMUNICATION DATA 30

PART VI – COST OF INTERCEPTION 31

PART VII – SAFEGUARDS 32

PART VIII – ADMISSIBILITY OF EVIDENCE 34

PART IX – SCHEDULE 35

Section III: Explanatory Notes to Model Legislative Text on Interception of Communications **37**

PART I – PRELIMINARY 38

PART II – INTERCEPTION OF COMMUNICATIONS 41

PART III – EXECUTION OF INTERCEPTION 54

PART IV – INTERCEPTION EQUIPMENT 56

PART V – DISCLOSURE OF STORED COMMUNICATIONS DATA 57

PART VI – COSTS OF INTERCEPTION 59

PART VII – SAFEGUARDS 59

PART VIII – ADMISSIBILITY OF EVIDENCE 60

PART IX – SCHEDULE 61

ANNEXES 63

Annex 1 Participants of the First Consultation Workshop for HIPCAR Project Working Group dealing with ICT Legislative Framework – Information Society Issues. 63

Annex 2 Participants of the Second Consultation Workshop (Stage B) for HIPCAR Project Working Group dealing with ICT Legislative Framework – Information Society Issues 65

Introduction

1.1. HIPCAR Project – Aims and Beneficiaries

The HIPCAR project[1] was officially launched in the Caribbean by the International Telecommunication Union (ITU) and the European Commission (EC) in December 2008, in close collaboration with the Caribbean Community (CARICOM) Secretariat and the Caribbean Telecommunications Union (CTU). The HIPCAR project is part of a global ITU-EC-ACP project encompassing also sub-Saharan Africa and the Pacific.

HIPCAR's objective is to assist CARIFORUM[2] countries in the Caribbean to harmonize their information and communication technology (ICT) policies, legislation and regulatory procedures so as to create an enabling environment for ICT development and connectivity, thus facilitating market integration, fostering investment in improved ICT capabilities and services, and enhancing the protection of ICT consumers' interests across the region. The project's ultimate aim is to enhance competitiveness and socio-economic and cultural development in the Caribbean region through ICTs.

In accordance with Article 67 of the Revised Treaty of Chaguaramas, HIPCAR can be seen as an integral part of the region's efforts to develop the CARICOM Single Market & Economy (CSME) through the progressive liberalization of its ICT services sector. The project also supports the CARICOM Connectivity Agenda and the region's commitments to the World Summit on the Information Society (WSIS), the World Trade Organization's General Agreement on Trade in Services (WTO-GATS) and the Millennium Development Goals (MDGs). It also relates directly to promoting competitiveness and enhanced access to services in the context of treaty commitments such as the CARIFORUM states' Economic Partnership Agreement with the European Union (EU-EPA).

The 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, St. Lucia, St. Vincent and the Grenadines, Suriname, and Trinidad and Tobago.

1.2. Project Steering Committee and Working Groups

HIPCAR has established a project Steering Committee to provide it with the necessary guidance and oversight. Members of the Steering Committee include representatives of Caribbean Community (CARICOM) Secretariat, Caribbean Telecommunications Union (CTU), Eastern Caribbean Telecommunications Authority (ECTEL), Caribbean Association of National Telecommunication Organisations (CANTO), Caribbean ICT Virtual Community (CIVIC), and International Telecommunication Union (ITU).

---

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-ACPproject carried out with funding from the European Union set at EUR 8 million and a complement of USD 500,000 by the International Telecommunicat(ITU). It is implemented ion Union by the ITU in collaboration with the Caribbean Telecommunications Union (CTU) and with the involvement of other organization in the region. (see www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html) .

2 The CARIFORUM is a regional organisation of fifteen independent countries in the Caribbean region (Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, Saint Christopher and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname, and Trinidad and Tobago). These states are all signatories to the ACP–EC Conventions.

In order to ensure stakeholder input and relevance to each country, HIPCAR Working Groups have also been established with members designated by the country governments – including specialists from ICT agencies, justice and legal affairs and other public sector bodies, national regulators, country ICT focal points and persons responsible for developing national legislation. This broad base of public sector participation representing different sectors allowed the project to benefit from a cross-section of views and interests. The Working Groups also include representatives from relevant regional bodies (CARICOM Secretariat, CTU, ECTEL and CANTO) and observers from other interested entities in the region (e.g. civil society, the private sector, operators, academia, etc.).

The Working Groups have been responsible for covering the following two work areas:

1. *ICT Policy and Legislative Framework on Information Society Issues*, dealing with six sub-areas: e-commerce (transactions and evidence), privacy & data protection, interception of communications, cybercrime, and access to public information (freedom of information).
2. *ICT Policy and Legislative Framework on Telecommunications*, dealing with three sub-areas: universal access/service, interconnection, and licensing in a convergent environment.

The reports of the Working Groups published in this series of documents are structured around these two main work areas.

1.3. Project Implementation and Content

The project's activities were initiated through a Project Launch Roundtable organized in Grenada, on 15-16 December 2008. To date, all of the HIPCAR beneficiary countries – with the exception Haiti – along with the project's partner regional organizations, regulators, operators, academia, and civil society have participated actively in HIPCAR events including – in addition to the project launch in Grenada – regional workshops in Trinidad & Tobago, St. Lucia, St. Kitts and Nevis, Suriname and Barbados.

The project's substantive activities are being led by teams of regional and international experts working in collaboration with the Working Group members, focusing on the two work areas mentioned above.

During *Stage I* of the project – just completed – HIPCAR has:

1. Undertaken assessments of the existing legislation of beneficiary countries as compared to international best practice and in the context of harmonization across the region; and
2. Drawn up model policy guidelines and model legislative texts in the above work areas, from which national ICT policies and national ICT legislation/ regulations can be developed.

It is intended that these proposals shall be validated or endorsed by CARICOM/CTU and country authorities in the region as a basis for the next phase of the project.

Stage II of the HIPCAR project aims to provide interested beneficiary countries with assistance in transposing the above models into national ICT policies and legislation tailored to their specific requirements, circumstances and priorities. HIPCAR has set aside funds to be able to respond to these countries' requests for technical assistance – including capacity building – required for this purpose.

1.4. Overview of the Six HIPCAR Model Policy Guidelines and Legislative Texts Dealing with Information Society Issues

Countries worldwide as well as in the Caribbean are looking for ways to develop legal frameworks addressing the needs of information societies with a view to leveraging the growing ubiquity of the World Wide Web as a channel for service delivery, ensuring a safe environment and the processing power of information systems to increase business efficiency and effectiveness.

Introduction

The Information Society is based on the premise of access to information and services and utilizing automated processing systems to enhance service delivery to markets and persons *anywhere in the world*. For both users and businesses the information society in general and the availability of information and communication technology (ICT) offers unique opportunities. As the core imperatives of commerce remain unchanged, the ready transmission of this commercial information creates opportunities for enhanced business relationships. This ease of exchange of commercial information introduces new paradigms: firstly, where information is used to support transactions related to physical goods and traditional services; and secondly, where information itself is the key commodity traded.

The availability of ICTs and new network-based services offer a number of advantages for society in general, especially for developing countries. ICT applications, such as e-Government, e-Commerce, e-Education, e-Health and e-Environment, are seen as enablers for development, as they provide an efficient channel to deliver a wide range of basic services in remote and rural areas. ICT applications can facilitate the achievement of millennium development targets, reducing poverty and improving health and environmental conditions in developing countries. Unhindered access to information can support democracy, as the flow of information is taken out of the control of state authorities (as has happened, for example, in Eastern Europe). Given the right approach, context and implementation processes, investments in ICT applications and tools can result in productivity and quality improvements.

However, the transformation process is going along with challenges as the existing legal framework does not necessary cover the specific demands of a rapidly changing technical environment. In cases where information supports trade in traditional goods and services, there needs to be clarity in how traditional commercial assumptions are effected; and in the instance where information is the commodity traded, there needs to be protection of the creator/ owner of the commodity. In both instances, there needs to be rationalization of how malfeasance is detected, prosecuted and concluded in a reality of trans-border transactions based on an intangible product.

The Six Inter-related Model Frameworks

The HIPCAR project has developed six (6) inter-related model frameworks that provide a comprehensive legal framework to address the above mentioned changing environment of information societies by guiding and supporting the establishment of harmonized legislation in the HIPCAR beneficiary countries.

Firstly a legal framework was developed to protect the right of users in a changing environment and thereby among other aspects ensuring consumer and investor confidence in regulatory certainty and protection of privacy, HIPCAR model legislative texts were developed to deal with considerations relating to: **Access to Public Information (Freedom of Information)** – geared to encouraging the appropriate culture of transparency in regulatory affairs to the benefit of all stakeholders; and **Privacy and Data Protection** – aimed at ensuring the protection of privacy and personal information to the satisfaction of the individual. This latter framework is focused on appropriate confidentiality practices within both the public and private sectors.

Secondly, in order to facilitate harmonization of laws with regard to the default expectations and legal validity of contract-formation practices, a HIPCAR model legislative text for **Electronic Commerce (Transactions)**, including electronic signatures was developed. This framework is geared to provide for the equivalence of paper and electronic documents and contracts and for the foundation of undertaking commerce in cyber-space. A legislative text dealing with **Electronic Commerce (Evidence)** – the companion to the Electronic Commerce (Transactions) framework, was added to regulate legal evidence in both civil and criminal proceedings.

To ensure that grave violations of the confidentiality, integrity and availability of ICT and data can be investigated by law enforcement, model legislative texts were developed to harmonise legislation in the field of criminal law and criminal procedural law. The legislative text on **Cybercrime** defines offences, investigation instruments and the criminal liability of key actors. A legislative text dealing with the **Interception of Electronic Communications** establishes an appropriate framework that prohibits the illegal interception of communication and defines a narrow window that enables law enforcement to lawfully intercept of communication if certain clearly defined conditions are fulfilled.

Developing the Model Legislative Texts

The model legislative texts were developed by taking into account key elements of international trends as well as legal traditions and best practices from the region. This process was undertaken to ensure that to the frameworks optimally meet the realities and requirements of the region of HIPCAR beneficiary countries for which and by which they have been developed. Accordingly, the process involved significant interaction with stakeholders at each stage of development.

The first step in this complex process was an assessment of existing legal frameworks within the region through a review of the laws related to all relevant areas.. In addition to enacted legislation, the review included, where relevant, bills which had been prepared but had yet to complete the process of promulgation. In a second step, international best practices (for example from United Nations, OECD, EU, the Commonwealth, UNCITRAL and CARICOM) as well as advanced national legislation (for example from the UK, Australia, Malta and Brazil, among others) were identified. Those best practices were used as benchmarks.

For each of the six areas, complex legal analyses were drafted that compared the existing legislation in the region with these benchmarks. This comparative law analysis provided a snapshot of the level of advancement in key policy areas within the region. These findings were instructive, demonstrating more advanced development in frameworks relating to Electronic Transactions, Cybercrime (or "Computer Misuse") and Access to Public Information (Freedom of Information) legislation than evidenced in the other frameworks.

Based upon the results of the comparative law analyses, the regional stakeholders developed baseline policy "building blocks" which – once approved by stakeholders – defined the bases for further policy deliberation and legislative text development. These policy building blocks reaffirmed some common themes and trends found in the international precedents, but also identified particular considerations that would have to be included in the context of a region consisting of sovereign small island developing states. An example of a major situational consideration which impacted deliberations at this and other stages of the process was the question of institutional capacity to facilitate appropriate administration of these new systems.

The policy building blocks were then used to develop customised model legislative texts that meet both international standards and the demand of the HIPCAR beneficiary countries. Each model text was then again evaluated by stakeholders from the perspective of viability and readiness to be translated into regional contexts. As such, the stakeholder group – consisting of a mix of legislative drafters and policy experts from the region – developed texts that best reflect the convergence of international norms with localised considerations. A broad involvement of representatives from almost all 15 HIPCAR beneficiary countries, regulators, operators, regional organizations, civil society and academia ensured that the legislative texts are compatible with the different legal standards in the region. However, it was also recognised that each beneficiary state might have particular preferences with regard to the implementation of certain provisions. Therefore, the model texts also provide optional approaches within the generality of a harmonised framework. This approach aims to facilitate widespread acceptance of the documents and increase the possibility of timely implementation in all beneficiary jurisdictions.

Interaction and Overlapping Coverage of the Model Texts

Due to the nature of the issues under consideration, there are common threads that are reflected by all six frameworks.

In the first instance, consideration should be given to the frameworks that provide for the use of electronic means in communication and the execution of commerce: **Electronic Commerce (Transactions), Electronic Commerce (Evidence), Cybercrime** and **Interception of Communications**. All four frameworks deal with issues related to the treatment of messages transmitted over communications networks, the establishing of appropriate tests to determine the validity of records or documents, and the mainstreaming of systems geared to ensure the equitable treatment of paper-based and electronic material in maltreatment protection, consumer affairs and dispute resolution procedures.

As such, there are several common definitions amongst these frameworks that need to take into account, where necessary, considerations of varying scope of applicability. Common concepts include: "electronic communications network" – which must be aligned to the jurisdiction's existing definition in the prevailing Telecommunications laws; "electronic document" or "electronic record" – which must reflect broad interpretations so as to include for instance audio and video material; and "electronic signatures", "advanced electronic signatures", "certificates", "accredited certificates", "certificate service providers" and "certification authorities" – which all deal with the application of encryption techniques to provide electronic validation of authenticity and the recognition of the technological and economic sector which has developed around the provision of such services.

In this context, **Electronic Commerce (Transactions)** establishes, among other things, the core principles of recognition and attribution necessary for the effectiveness of the other frameworks. Its focus is on defining the fundamental principles which are to be used in determining cases of a civil or commercial nature. This framework is also essential in defining an appropriate market structure and a realistic strategy for sector oversight in the interest of the public and of consumer confidence. Decisions made on the issues related to such an administrative system have a follow-on impact on how electronic signatures are to be procedurally used for evidentiary purposes, and how responsibilities and liabilities defined in the law can be appropriately attributed.

With that presumption of equivalence, this allows the other frameworks to adequately deal with points of departure related to the appropriate treatment of electronic information transfers. The **Cybercrime** framework, for example, defines offences related to the interception of communication, alteration of communication and computer-related fraud. The **Electronic Commerce (Evidence)** framework provides a foundation that introduces electronic evidence as a new category of evidence.

One important common thread linking **e-Transactions** and **Cybercrime** is the determination of the appropriate liability and responsibility of service providers whose services are used in situations of electronically mediated malfeasance. Special attention was paid to the consistency in determining the targeted parties for these relevant sections and ensuring the appropriate application of obligations and the enforcement thereof.

In the case of the frameworks geared to improving regulatory oversight and user confidence, the model texts developed by HIPCAR deal with opposite ends of the same issue: whereas the **Access to Public Information** model deals with encouraging the disclosure of public information with specified exceptions, the **Privacy and Data Protection** model encourages the protection of a subset of that information that would be considered exempted from the former model. Importantly, both these frameworks are geared to encouraging improved document management and record-keeping practices within the public sector and – in the case of the latter framework – some aspects of the private sector as well. It is however notable that – unlike the other four model texts – these frameworks are neither applicable exclusively to the electronic medium nor about creating the enabling framework within which a new media's considerations are transposed over existing procedures. To ensure consistency, frameworks are instead geared to regulating the appropriate management of information resources in both electronic and non-electronic form.

There are a number of sources of structural and logistical overlaps which exist between these two legislative frameworks. Amongst these is in the definition of the key concepts of "public authority" (the persons to whom the frameworks would be applicable), "information", "data" and "document", and the relationship amongst these. Another important form of overlap concerns the appropriate oversight of these frameworks. Both of these frameworks require the establishment of oversight bodies which should be sufficiently independent from outside influence so as to assure the public of the sanctity of their decisions. These independent bodies should also have the capacity to levy fines and/or penalties against parties that undertake activities to frustrate the objectives of either of these frameworks.

In Conclusion

The six HIPCAR 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 both the most current international standards as well as the demands of small islands developing countries in general and – more specifically – those of HIPCAR's beneficiary countries. 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. Although the focus has been on the needs of countries in the Caribbean region, the aforementioned model legislative texts have already been identified as possible guidelines also by certain countries in other regions of the world.

Given the specific and interrelated natures of the HIPCAR model texts, it will be most advantageous for the project's beneficiary countries to develop and introduce legislation based on these models in a coordinated fashion. The Electronic Commerce models (Transactions and Evidence) will function most effectively with the simultaneous development and passage of Cybercrime and Interception of Communications frameworks, as they are so closely related and dependent on each other to address the concerns of robust regulatory development. Similarly, the Access to Public Information and the Privacy and Data Protection frameworks consist of such synergies in administrative frameworks and core skill requirements that simultaneous passage can only strengthen both frameworks in their implementation.

In this way there will be optimal opportunity created to utilise the holistic frameworks that are established in the region.

1.5. This Report

This report deals with Interception of Communications, one of the work areas of the Working Group on the ICT Policy and Legislative Framework on Information Society Issues. It includes Model Policy Guidelines and a Model Legislative Text including Explanatory Notes that countries in the Caribbean may wish to use when developing or updating their own national policies and legislation in this area.

Prior to drafting this document, HIPCAR's team of experts – working closely with the above Working Group members – prepared and reviewed an assessment of existing legislation on information society issues in the fifteen HIPCAR beneficiary countries in the region focusing on six areas: Electronic Transactions, Electronic Evidence in e-Commerce, Privacy and Data Protection, Interception of Communications, Cybercrime, and Access to Public Information (Freedom of Information). This assessment took account of accepted international and regional best practices.

This regional assessment – published separately as a companion document to the current report[3] – involved a comparative analysis of current legislation on Interception of Communications in the HIPCAR beneficiary countries and the identification of potential gaps in this regard, thus providing the basis for the development of the model policy framework and legislative text presented herein. By reflecting national, regional and international best practices and standards while ensuring compatibility with the legal traditions in the Caribbean, the model documents in this report are aimed at meeting and responding to the specific requirements of the region.

The model legislative text on Interception of Communications was developed in three phases: (1) the drafting of an assessment report; (2) the development of model policy guidelines; and (3) the drafting of the model legislative text. The assessment report was prepared in two stages by HIPCAR consultants. The first stage was carried out by Ms. Karen Stephen-Dalton, and the second stage by Mr. Gilberto Martíns de

[3] See "ICT Policy and Legislative Framework on Information Society Issues – Interception of Communications: Assessment Report on the Current Situation in the Caribbean" available at www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/

Almeida. Following this, the draft model policy guidelines were prepared by Mr. Martíns de Almeida, and then reviewed, discussed and finalized by the HIPCAR Working Group on Information Society Issues during the project's First Consultation Workshop for the above Working Group held in Saint Lucia on 8-12 March 2010. Based on the model policy guidelines, the HIPCAR consultant Dr. Marco Gercke prepared the draft model legislative text, which was also reviewed, discussed and finalized by the above Working Group during the project's Second Consultation Workshop held in Barbados on 23-26 August 2010 (see Annexes). The explanatory notes to the model legislative text were prepared by Dr. Gercke addressing, *inter alia*, the points raised at the second workshop. The documents were endorsed by a broad consensus at these workshops. The HIPCAR Project Steering Committee and the Project Management Team oversaw the process of developing these documents.

Following this process, the documents were finalized and disseminated to all stakeholders for consideration by the governments of the HIPCAR beneficiary countries.

1.6. The Importance of Effective Policies and Legislation on Interception of Communications

In the context of Information Society, where communications[4] 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.

In accordance with ITU's Toolkit for Cybercrime Legislation[5], "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."[6]

Such a definition explains the broad scope of "interception" as well of the "communication" subject to it, which includes "content" (information communicated) and "traffic" (data relating to communication)[7]. 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.

---

4 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."

5 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.

6 Section 1 – Definitions, item "k".

7 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."

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"[8] and of "location data"[9] 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.*[10]

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 and Jamaica – to enact legislation that requires electronic communications service providers to be capable of carrying out lawful interception and to regulate interception of communications activities.

For interception of communications to be lawful it must be conducted in accordance with national law, which may regulate either private or official interception of 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 labor 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.

---

8 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."

9 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".

10 Notes on OECS Interception of Communications Bill, page 6 found at www.//unpan1.un.org/intradoc/groups/public/documents/TASF/UNPAN024635.pdf

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).

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"*[11] is recommended.

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

Section I:
Model Policy Guidelines – Interception of Communications

Following, are the Model Policy Guidelines that a country may wish to consider in relation to Interception of Communications.

1. CARICOM/CARIFORUM COUNTRIES SHALL AIM TO ESTABLISH NECESSARY COMMON INTERPRETATIONS FOR KEY TERMS ASSOCIATED WITH INTERCEPTION OF COMMUNICATION

- There shall be proper definition on "interception", "communications", "data", "content", "traffic", "content data", "traffic data", "location data".
- There shall be sufficiently broad wording in the definition of these terms, coupled with a list of illustrative examples.
- There shall be clear definition on the kind of information (text, visual, sound) and scope of media subject to interception of communication, so that it encompasses electronic or non-electronic documents, tapes, films, sound recording, images, and others, either produced by a public party or by a private party, at any time.
- To the extent compatible with national security concerns, there shall be public campaign that aims to develop awareness on communication subject to interception, and explaining the public policies which justify and address it.

2. CARICOM/CARIFORUM COUNTRIES SHALL AIM TO ESTABLISH THE NECESSARY FRAMEWORK TO DEFINE THE PUBLIC OR PRIVATE ORIGIN, AND ROLE, OF THE PARTIES IN CHARGE OF MANAGING INTERCEPTION OF COMMUNICATION[12]

- There shall be provision in law which explicitly states what is the role of "public authorities" (such as Law Enforcement Agencies) and of "private bodies" (such as ISPs and Telecom companies) in the context of interception of communication.
- There shall be provision establishing that private parties are required to cooperate with public authorities in interception of communication as determined by applicable legislation (procedural criminal laws, national security laws), to the extent legally allowed.
- There shall be regulation providing room for recognition and incorporation of commonly accepted technical standards which address electronic and/or telephonic monitoring, and which may be instrumental for interception of communication.
- There shall be public policy harmonizing interception of communication and privacy rights, freedom of information, intellectual property, and other public policies which deal with fostering production, keeping and release of information.

[12] There shall be public policy encouraging institutional cooperation (for instance, with industry and with commerce) for development or use, as the case may be (and, to the extent necessary, sharing) databases and other mechanisms of storage or publication of data which are relevant to achieving the goals of interception of communication.
There shall be constant monitoring on new challenges to interception of communication (such as steganography, cloud computing, and others).

- There shall be formal criteria established on how to address requests and orders for interception of communication coming from abroad.
- There shall be formal criteria, and training, for carrying out interception of communication in a manner capable of being accepted as electronic evidence.

3. CARICOM/CARIFORUM COUNTRIES SHALL DEFINE THE LEGAL MANDATES AND THE STANDARDS TO WHICH INTERCEPTION OF COMMUNICATION SHALL BE BOUND

- The law/legal mandate shall be enabling in nature and refrain from being overly prescriptive in its provisions.
- The law/legal mandate shall state that no communication shall be intercepted unless there is public interest for it, and that interception is carried out in accordance with legal procedures, standards and practices.
- The law/legal mandate shall specify which are the constitutional grounds of interception of communication, in order to establish its weight vis-à-vis other constitutional rights or principles.
- The law/legal mandate shall provide for the criteria which must guide selection of electronic searches of communication to be intercepted.
- The law/legal mandate shall determine which are the acceptable patterns for implementation of interception of communication, taking into account search duration, scope of search, filter mechanisms, maximum time for keeping intercepted communication, security for storing intercepted communication, proper discarding, and other procedures.
- The law/legal mandate may establish different treatment for content data, traffic data, and location data.
- The law/legal mandate shall determine that the management of interception of communication be guided by the objectives of conformity with legal principles, efficiency, effectiveness and records tracking.
- The law/legal mandate shall define which communications (such as terrorism, counter-intelligence) may be subject to special interception procedures and administrative structures.

4. CARICOM/CARIFORUM COUNTRIES SHALL DEFINE EXEMPTIONS FROM COMPLIANCE WITH INTERCEPTION OF COMMUNICATION

- The law/ legal mandate shall provide for exemptions clearly and narrowly drawn, in order to avoid wide-ranging exemptions, which could defeat the purposes of interception of communication.
- The law/ legal mandate shall define that communications (such as banking, medical, and others) are exempt from interception unless there is judicial order granting authorization for interception.
- The law/ legal mandate shall develop awareness on criteria which harmonize interception of communication and various kinds of secrecy (banking, tax, mail, professional, judicial, and others).
- The law/ legal mandate shall state that where the public interest in keeping a communication secret is greater than the public interest in its interception, its interception shall be deemed not allowed.
- The law/ legal mandate shall establish that interception of communication is consistent with public policy on freedom to encrypt communication (and to use other means of disguising flow of communication, such as re-mailing).

Section I

5. CARICOM/CARIFORUM COUNTRIES SHALL ESTABLISH PROCEDURES FOR OVERSIGHT, ENFORCEMENT, REVIEW AND APPEAL IN CONNECTION WITH INTERCEPTION OF COMMUNICATION

- The law/legal mandate shall establish procedures for oversight, enforcement, review and appeal in connection with interception of communication.
- The law/legal mandate shall establish that both the applicant and the public authority shall have a right of appeal to the Courts against decisions of the administrative body.
- The law/legal mandate shall establish time lines so that the response to requests and the provision of information are not delayed beyond reasonable time.
- The law/legal mandate shall establish sanctions for the failure to comply with duties and obligations relating to interception of communication.

6. CARICOM/CARIFORUM COUNTRIES SHALL ESTABLISH THE FRAMEWORK OF INTERCEPTION OF COMMUNICATION IN CONJUNCTION WITH PUBLIC POLICIES ON RELATED MATTERS

- The law/legal mandate shall regulate interception of communication in a way consistent with public policy on national security.
- The law/legal mandate shall regulate interception of communication in a way consistent with public policy on cybercrime.
- The law/legal mandate shall regulate interception of communication in a way consistent with public policy on freedom of information.
- The law/legal mandate shall regulate interception of communication in a way consistent with public policy on privacy and on data protection.
- The law/legal mandate shall regulate interception of communication in a way consistent with relevant public policy on censorship.
- The law/legal mandate shall regulate interception of communication in a way consistent with public policy on information security.
- The law/legal mandate shall regulate interception of communication in a way consistent with public policy on intellectual property.
- The law/legal mandate shall regulate interception of communication in a way consistent with public policy on freedom of broadcasting.
- The law/legal mandate shall regulate interception of communication in a way consistent with public policy on *habeas data* where applicable.

Section II:
Model Legislative Text –
Interception of Communications

Following, is the Model Legislative Text that a country may wish to consider when developing national legislation relating to Interception of Communications. This model text is based on the Model Policy Guidelines outlined previously.

Arrangement of Sections

PART I – PRELIMINARY 17
1. Short Title 17
2. Objective 17
3. Definitions 17
4. Applications 18

PART II – INTERCEPTION OF COMMUNICATIONS 18
5 Prohibition of Interception of Communications 18
6. Application for the Interception Warrant 19
7. Application Disclosure 20
8. Issuance of the Interception Warrant 21
9. Scope and form of Interception Warrant 22
10. Duration and Renewal of Interception Warrant 23
11. Modification of Interception Warrant 23
12. Revocation of Interception Warrant 24
13. Consequences of Revocation 24
14. Urgent Application 24
15. Report on Progress 25
16. Final Report 25

PART III – EXECUTION OF INTERCEPTION 26
17. Execution of Interception Warrant 26
18. Entry of Premise for the Execution of Interception Warrant 26
19. Duty to Provide Assistance 26
20. Failure to Assist 27
21. Confidentiality of Intercepted Communication 27
22. Failure to Keep Information on Interception Confidential 27
23. Destruction of Records 27
24. Failure to Destroy Records 28

PART IV – INTERCEPTION EQUIPMENT 28
25. Listed Equipment with Interception Capabilities 28
26. Prohibition of Manufacture, Possession and Use of Listed Equipment with Interception Capacities 29
27. Use of Equipment Without Authorization 29
28. Authorization to Use Listed Equipment with Interception Capabilities 29

PART V – DISCLOSURE OF STORED COMMUNICATION DATA 30
29. Prohibition of Access to Stored Computer Data 30
30. Disclosure of Stored Communication Data 30
31. Failure to Keep Information on Disclosure Order Confidential 31

PART VI – COST OF INTERCEPTION 31
32. Allocation of Costs 31

PART VII – SAFEGUARDS 32
33. Professional Secrecy 32
34. Monitoring of Communications Interception 32
35. Independent Commissioner on Interception of Communications 33

PART VIII – ADMISSIBILITY OF EVIDENCE 34
36. Admissibility of Intercepted Communications as Evidence 34
37. Inadmissibility of Intercepted Communications as Evidence 34

PART IX – SCHEDULE 35
38. Amendment of Schedule 35
39. Regulations 35

Section II

PART I – PRELIMINARY

Short Title 1. This Act may be cited as the Interception of Communications Act, and shall come into force and effect [on xxx/ following publication in the *Gazette*].

Objective 2. [This is an Act 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].

Definitions 3. (1) Agency means an [interception agency] or [another 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 [number of] 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 [name of the publication] subject to affirmative resolution.

(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 warrant 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] [name of the ministry].

[(15) Person includes a body corporate or an unincorporated body.].

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

Application 4. (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 [State].

PART II – INTERCEPTION OF COMMUNICATIONS

Prohibition of Interception of Communications 5. (1) A person who intentionally intercepts any communication during its transmission commits an offence punishable, on conviction to a fine not exceeding [amount], or by imprisonment for a period not exceeding [period], or both.

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

a. The communication is intercepted in accordance with an interception warrant issued pursuant to Section 8 by a [judge];

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 in relating to the use of those services;

e. The interception is of a communication made through a communications network that is configured 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.

Note: A country may restrict the criminalisation by establishing addition requirements.

Application for the Interception Warrant

6. (1) An [authorised officer] [Director of Public Prosecutions on behalf of an authorised officer] may apply ex parte to a [judge] for a warrant 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 warrant must be in written form and be accompanied by affidavit containing the following:

a. The name of the authorised officer [on behalf of which the application is made];

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

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

d. Sufficient information for a [judge] to issue an interception warrant 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 warrant 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].

(3) Where an interception warrant 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 warrant or the renewal or modification thereof shall be;

a. placed in a packet and sealed by the [judge] 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] may authorise.

(5) The records referred to in subsection (5), may be opened if a [judge] orders and 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 [amount] or by imprisonment for a period not exceeding [period], or both.

Application Disclosure

7. (1) Any person who discloses the existence of an application for an interception warrant, other than to the authorised officer, commits an offence punishable, on conviction, for a fine not exceeding [amount] or by imprisonment for a period not exceeding [period], 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 this 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 Warrant

8. (1) A [judge] shall authorise interception and issue an interception warrant if he or she is satisfied that:

a. the interception warrant is necessary

i. in the interests of national security; or

ii. for the prevention or detection of any offence specified in the Schedule, where there are reasonable grounds 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] to be equivalent to those in which he or she would issue an interception warrant 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 warrant;

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 warrant.

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

Section II

Scope and form of Interception Warrant

9. (1) An interception warrant 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 warrant;

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

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

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

i. a particular individual specified in the interception warrant;

ii. a particular address specified in the interception warrant;

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

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

(3) An interception warrant may authorise entry on any premises specified in the warrant as it is referred to in the Section 18 for the purpose of installing, maintaining, using or recovering any equipment used to intercept communications specified in the warrant.

(4) An interception warrant 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 warrant;

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

d. when interception warrant authorises the entry on premises under the 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 warrant may contain ancillary provisions that are necessary to secure its implementation in accordance with this Act.

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

Note: Countries may – depending on their legal traditions – require additional procedural safeguards.

(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

10. (1) An interception warrant shall be valid for such period, not exceeding [*90*] days, as the [judge] shall specify in the warrant, 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] may, on an application for the renewal of an interception warrant made by an [authorised officer] [*Director of Public Prosecutions* on behalf of an authorised officer] renew an interception warrant at any time before the warrant (or any current renewal of the warrant) has expired.

(3) An application for the renewal of an interception warrant 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 warrant.

(4) Every application for the renewal of an interception warrant 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 warrant, 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 warrant shall be supported by such other information as the [judge] may require.

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

(7) Every renewal of an interception warrant shall be valid for such period, not exceeding [*90*] days, as the [judge] 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 10, it appears to the authorised officer to whom the warrant is issued, or a person acting on his or her behalf, that an interception warrant is no longer necessary, he or she shall make an application to [judge] for the revocation of the interception warrant.

Modification of Interception Warrant

11. (1) A [judge] may modify any of the provisions of an interception warrant at any time, after hearing representations from the [*Authorised officer/ Director of Public Prosecutions* acting on behalf of an authorised officer] and 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 warrant shall be made in accordance with Section 6 and shall contain information referred to in subsection (2) of Section 6.

Revocation of Interception Warrant

12. (1) A [judge] who issued an interception warrant [or, if he or she is not available, any other [judge] entitled to issue such a warrant] may revoke the interception warrant, if

a. the authorised officer fails to submit a report in accordance with Section 15, if applicable; or

b. the [judge] upon receipt of a report submitted pursuant to Section 15 is satisfied that the objectives of the interception warrant have been achieved; or

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

d. the conditions of the application referred to in subsection (1) of Section 8 have changed in a way that an application would not be possible anymore.

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

(3) If the interception warrant 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 warrant relates under subsection (3) of Section 9, any intercepted device, which was installed under the same subsection.

Consequences of Revocation

13. Where an interception warrant issued in accordance with this Act is revoked in accordance with Section 12, the contents of any communication intercepted under that warrant 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

14. (1) Where a judge 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 warrant; and

b. If satisfied that an interception warrant is necessary he shall issue or an interception warrant 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 authorised officer justifies the making of an oral application.

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

a. there are reasonable grounds to believe that the interception warrant 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] [Director of Public Prosecutions applying on behalf of the authorised officer] to make a written application for the issuing of the interception warrant, applied for.

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

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

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

(7) Where an interception warrant is issued under this section, the [authorised officer] [*Director of Public Prosecutions* on behalf of the authorised officer] shall within [*48*] hours of the time of the issue submit to the [judge] 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 warrant; under this section, the [judge] shall review his or her decision to issue the interception warrant.

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

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

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

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

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

Report on Progress

15. A [judge] who has issued an interception warrant, 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 warrant, to report to him or her in writing on:

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

b. any other matter which the [judge] considers necessary.

Final Report

16. (1) As soon as practicable after an interception warrant has expired, the authorised officer who applied for it, shall make a written report to the [judge] who granted the interception warrant, or if that [judge] is unable

to act to another [judge], on the manner in which the power conferred by the interception warrant 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 warrant have been destroyed in accordance with Section 23 and, if not, why they have not been destroyed.

PART III – EXECUTION OF INTERCEPTION

Execution of Interception Warrant

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

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

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

(4) An authorised officer or person acting under or in compliance with an interception warrant or who aids in good faith a person who he believes on reasonable grounds is acting in accordance with such authorisation does not incur any criminal or civil liability for anything reasonably done further to the interception warrant.

Entry of Premise for the Execution of Interception Warrant

18. If an interception warrant contains a permission that an authorised officer enters on premises pursuant to subsection (3) Section 9, an authorised officer may at the time specified in the interception warrant enter the premises and perform acts that he or she is authorised to perform in accordance with the interception warrant.

Duty to Provide Assistance

19. (1) A person which provides communications services shall permit, and assist if required and reasonable, an authorised officer to exercise interception warrant.

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

Failure to Assist

20. A person, who intentionally and without lawful excuse or justification fails to permit or assist an authorised officer in the execution of interception as specified in subsection (1), (2) of Section 19, commits an offence punishable, on conviction, to a fine not exceeding [amount] or by imprisonment for a period not exceeding [period], or both.

Confidentiality of Intercepted Communication

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

a. to limit to the minimum that is necessary for the purposes for which the interception warrant 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 23.

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

a. existence and the contents of the interception warrant;

b. details of the issue of the interception warrant 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 warrant;

e. all intercepted materials with any related communications data.

Failure to Keep Information on Interception Confidential

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

Destruction of Records

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

(2) Any records of the information obtained from the interception of communications in pursuance of an interception warrant, being information that relates to wholly or partly and directly or indirectly to the aim of the interception warrant 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] in accordance with section 16 shall state whether or not subsection (2) has yet been complied with, and, if it has not, the [judge] shall give such directions relating to the eventual destruction of the record as the [judge] thinks necessary to ensure compliance with that subsection, including a requirement that the [judge] be advised when the record has been destroyed.

Failure to Destroy Records

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

PART IV – INTERCEPTION EQUIPMENT

Listed Equipment with Interception Capabilities

25. [(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 draft notice and the notice under subsection (1).

(6) Subsection (4) does not apply if:

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.

(7) Any notice under subsection (1) shall, before publication thereof in the [*Gazette*] be by means of affirmative resolution.]

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

26. [(1) Subject to subsection (2) of this section and Section 27, a person shall not assemble, possess, sell, purchase and use any listed equipment.

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

Use of Equipment Without Authorization

27. [(1) A person who intentionally and without lawful excuse or justification contravenes or fails to comply with the requirements of Section 26, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], 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 shall be forfeited.

Note: A country may include provision allowing termination of license in case if communications provider intentionally and without lawful excuse or justification contravenes or fails to comply with the requirements of Section 26.].

Authorization to Use Listed Equipment with Interception Capabilities

28. [(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 26 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 V – DISCLOSURE OF STORED COMMUNICATION DATA

Prohibition of Access to Stored Computer Data

29. (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 [period], or a fine not exceeding [amount], 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 a interception warrant; or

c. stored communication is accessed based on a under other warrants and orders issued in accordance to procedural legislation.

Disclosure of Stored Communication Data

30. (1) Where it appears to the [designated person] [judge] that a person providing communications service is or may be in possession of, or capable of obtaining, any communications data, the [designated person] [judge] 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 [designated person] [judge] 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 authorised officer.

(3) A [designated person] [judge] 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 purposed 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 authorised officer specified in the notice for the purpose of;

i. ensuring that the notice is complied with, or obtaining legal advice or representation in relation to the 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

31. 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 30, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.].

PART VI – COST OF INTERCEPTION

Allocation of Costs

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

(2) A country may establish the model of reimbursement of direct costs incurred by communications provider in respect of personnel and administration which are required for purposes of providing assistance in execution of interception warrant.

PART VII – SAFEGUARDS

Professional Secrecy

33. [If the evidence obtained by the interception of communication have been privileged by virtue of[law] protecting:

a. [medical secrecy];

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

c. [bank secrecy];

d. [financial secrecy];

e. [any other secrecy that country want to protect by the virtue of law]

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

Monitoring of Communications Interception

34. [(1) Independent Monitoring Authority shall be created 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) Instead of creating separate Independent Monitoring Authority, a country may vest any authority that is:

a. not actively involved in the investigation process; and

b. has the capacity to perform necessary functions to supervise the interception with the functions of the Independent Monitoring Authority.

(3) An authorised officer shall in no more than [7] days after submitting a Final Report (Section 16) submit the following information to the Independent Monitoring Authority for the purpose of keeping Registry of Interception Warrants:

a. date of issue of the warrant;

b. [judge] who issued the warrant;

c. agency to which the warrant was issued; and

d. period for which the warrant was in force.

(4) Independent Monitoring Authority:

a. keeps the Registry of Interception Warrants, recording information specified in subsection (3) of Section 34; and

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

(5) Independent Monitoring Authority may, by written notice given to the [chief officer of the eligible authority], require the [eligible 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].

Section II

Independent Commissioner on Interception of Communications

35. [(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 purpose 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 Warrants; and

d. may require an officer of the [agency] to give the Independent Commissioner such information as the Registry of Interception Warrants 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 Independent Commissioner while exercising the duties under the subsections (3) and (4) shall be answered in [*7*] days.

(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 investigation made under the subsection (6) the Independent Commissioner discovered any breach of this Act, he or she can issue binding determination requiring to eliminate the violate or to stop activity that contravenes this Act.

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

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

(10) Individual or public authority has the right of appeal to the Courts against decisions of the Independent Commissioner.].

PART VIII – ADMISSIBILITY OF EVIDENCE

Admissibility of Intercepted Communications as Evidence

36. [(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 warrant or an emergency interception warrant 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 that person's intention to do so, together with

a. a transcript of the private communication where that person intends to adduce it in the form of a recording, or a written statement setting forth the full particulars of the communication where that person 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 warrant or an emergency permit, 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

37. Where a communication intercepted by means of an interception device otherwise than in pursuance of an interception warrant or emergency interception warrant 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.].

Section II

PART IX – SCHEDULE

Amendment of Schedule 38. (1) The Minster may, by order, add to or delete from list of offences contained in the Schedule.

(2) An order made under Subsection (1) shall be a subject of affirmative resolution.

Regulations 39. (1) The minister may make regulations to give effect to the purpose of this Act.

(2) Regulations made under Subsection (1) shall be a subject of affirmative resolution of the Parliament.

SCHEDULE

(Section 8 (1) (a) (ii))

(1) [Murder or Manslaughter or treason].

(2) [Kidnapping or abduction].

(3) [Money laundering] contrary to the [Proceeds of Crime and Money Laundering (Prevention) 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 [section of the Firearms Act].

(9) An offence contrary to [section of 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.

Section III:
Explanatory Notes to Model Legislative Text on Interception of Communications

INTRODUCTION

1. This legislative text provides a model legal framework for a lawful interception of communications. The principal aims of this legislative text 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. This legislative text was prepared and adopted in accordance with the Model Policy Guidelines of the First Consultation Workshop of HIPCAR Working Group 1 on Information Society Issues.
3. These notes are prepared to explain the content of the model legislative text and need to be read in conjunction with the legislative text. They explain the importance of the provisions and, where applicable, reflect the discussion within the HIPCAR[13] Working Group[14] and Policy Guidelines 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.
4. The legislative text consists of nine parts:
   - **Part I** provides definitions and sets the objective of the legislative text;
   - **Part II** prohibits unlawful interception and establishes the limited set of conditions when 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 warrant, and the rules for duration, renewal, and revocation of warrants;
   - **Part III** develops a framework for 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;

---

13 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).

14 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.

- **Part VI** covers the issue of the allocation of costs that incur 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 legislative text.

COMMENTARY ON SECTIONS

PART I – PRELIMINARY

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

6. Sections 2 and 3 raised a discussion within the HIPCAR Working Group with regard to the style of legislative drafting within different jurisdictions. It was discussed whether the Section with definitions should be placed prior to the section providing objectives of the model legislative text. It was agreed that this question should be left to the individual state.

Section 3. Definitions

7. Terms in square brackets indicate the choices individual states have within the implementation of the legislation. Due to the existing enactments or its domestic legal system, a country may decide to choose another term for the words provided in square brackets.

8. The definition of Agency provided by subsection (1) enables the determination of the agency that will intercept to the beneficiary states. There was a debate within the Working Group if there shall be any recommendations with regard to the bodies that shall be granted such power. However, it was agreed that each country decides itself which agency should be granted with the capability to intercept.

9. The same choice is provided by subsection (2), which constructs the definition for an authorised officer. While it is very important to determine and define, who will be able to apply for an interception warrant and will carry out interception procedures, the choice is left to the beneficiary states, which will determine their own list of persons that are granted with the permission to request an authorisation to intercept communications.

10. Subsection (3) defines what communication means for the purpose of constructing a framework that regulates interception. For the legislative text that prohibits interception of communications, it is very important, firstly, to draft the definition technology neutral, and, secondly, to avoid any limitations that could exclude relevant types of communications from the ban on interception. That is why 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.

11. The definition of **communication provider** is constructed in the subsection (4) for the purpose of imposing the obligation to intercept communications. Since this Act provides the possibility to oblige operators to intercept communications in accordance with the warrant, in order to protect small communications providers that are not capable to carry out an interception, a country shall define the number of customers that are served by a communications provider in order to provide the court with the possibility to oblige communications operator (provider) to intercept.

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

13. It was agreed that the 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.

14. 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 the 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 purpose of this Act.

15. The Working Group also discussed the definition of communications with regard to the scope of the legislative text. The question was raised whether the 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 to the interception of the postal services.

16. The definition of **communication service** provided by subsection (6) is important to make a distinction between communications network and communications services. It establishes that for the purpose of this legislative text, 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.

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

18. Subsection (9) provides one of the main definitions of this legislative text. In order to determine what is prohibited and regulated by this legislative text, 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.

19. Subsection (10) is developed to define **intercepted communication** in order to distinguish it from, for instance, stored communications data. Even if communications is stored after the interception is made, the main approach to define 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.

20. Since the definition of interception includes the reference to the term 'interception device', the latter is defined by subsection (11). 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 if 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.

21. 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.

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

23. For the purpose 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) that 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. A country is advised to include the definition of listed equipment only if it follows the approach suggested by Section 25 of this legislative text.

24. The definition of **Minister** is provided to give states a possibility to define a Ministry that will develop regulations with regard to the interception of communications. This can for instance be the Ministry of National Security, or any other ministry that is granted the power to deal with interception issues.

25. The definition of a **Person** provided by subsection (15) was drafted by the Working Group in order to include both a body corporate and an unincorporated body.

26. 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 model legislative text provides different frameworks for granting capability to intercept communication that is being transmitted and provide access to the stored communications. It is essential to draw a clear line between these two procedures and two different types of communications in terms of interception.

1.7. Section 4: Application

27. The main purpose of this Section is to determine the scope of the model legislative text, 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 right of individual. Subsection (1) thus provides that nothing in this legislative text shall be construed as requiring or prohibiting the anonymity or encryption of communications. This provision is developed to prevent the possibility to use the legislative text 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.

28. 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 legislative text would 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 this 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.

29. Subsection (2) is constructed to make a distinction between interception of communications under this legislative text 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 the Section 4 specifies that the legislative text does not apply if communication is a subject to special interception procedures and administrative structures under other law. This means that if there is any other regulation that 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, the legislative text does not apply to these special interception procedures.

PART II – INTERCEPTION OF COMMUNICATIONS

30. This part of the model legislative text pursues the main aims of the document: firstly, to prohibit an unlawful interception of communications and, secondly, to establish the limited number of circumstances and strict conditions in which interception can be authorised.

31. The approach on prohibition of interception of communications taken by this legislative text is similar to many regional and national approaches in this area, such as OESC[15] Model Law, legislation of Australia, Hong Kong, South Africa, and the United Kingdom. Criminalisation of unlawful interception in abovementioned national jurisdictions is usually followed by provisions establishing the lawful excuse for the interception and regulating the authorisation process.

32. 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 UK establish the right to intercept without prior court authorisation. Finally, interception can be authorised for the 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 warrants;
- determines the scope, form and duration of interception warrant as well as ground for its extension and revocation.

[15] Organisation of Eastern Caribbean States

33. 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 interference 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 5: Prohibition on Interception of Communications

34. Section 5 creates an offence of unlawful interception and explains the circumstances that can justify the lawfulness of the interception. This approach allows implementing strict safeguard first and then limiting the interception to serious crimes and national security issues.

35. 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 legislative text. 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 without 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.

36. 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.

37. Subsection (2) (a) warrants the right to intercept in accordance with the authorisation obtained in court. This model legislative text regulates the process of obtaining and executing such an authorisation.

38. Subsection (2) (b) defines that interception is lawful when there is a reasonable ground to believe that the party of communication has given consent for it. This provision is important to exclude consensual interception from the scope of the legislative text. This model legislative text 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 own communications protects private interest of the person, particularly in commercial and business context. A party of 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 corresponds with the right to wiretap own communications as known in some jurisdictions.

39. Subsection (2) (c) excludes stored communications data acquired under the 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 id not commenced or has completed passing through communications network.

40. 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 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 shall be exempted from criminalisation.

41. 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.

42. 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 that are not initially safeguarded by privacy right since they are readily accessible to the public.

43. Subsection (2) (f) makes an exemption for interception of communications received and transmitted within network that serve the need of the 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.

44. The Working Group discussed if 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.

45. 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.

46. 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 6. Application for the Interception Warrant

47. Section 6 aims to establish the procedure for the initial application to authorise interception.

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

49. The warrant 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 interference is taking place. Secondly, it provides the intruder with a written permission which he or she can produce only under certain conditions. Furthermore, a warrant 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 warrant system has advantages in cases where physical intrusion into premises is involved.

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

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

52. The issue of the authorisation by 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 warrants sanctioning interception shall be authorised only by the courts, with no distinction made between warrants relating to law enforcement and those relating to national security. Although some countries distinguish between warrants according to whether they relate to crime (for the judiciary) or public security (for the executive), the comprehensive approach that strikes a balance between the public interest and the rights of the individual is to require all authorisation are authorised by court.

53. 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 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 warrant will have to consider the matter carefully. It will also decrease the possibility of the abuse of power.

54. With regard to the application process, the working group changed subsection 6 (1) by adding that application is made ex parte. This amendment is necessary to enable an authorised officer to apply for the interception warrant based entirely on evidence represented by him or her without notifying the person whose communications shall be intercepted.

55. There was also a substantial discussion in the Working Group on the eligibility of the authorised officer to apply for the interception warrant. Many national approaches including regional bill (such as the OESC 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 and additional mechanism of checks and balance. 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.

56. Subsection (2) of Section 6 defines that an application for an interception warrant 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 to 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 certain requirements and, since all documents must be provided in written form, to guarantee the transparency of the application process.

57. 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 warrant 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.

58. 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, OESC Model Law) while other jurisdictions follow the approach of hearing viva voce evidence representation (e.g. Denmark, Finland, Slovenia).

59. 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 application and to prevent the opportunity for abuse.

60. In order to enable a court to make an informed decision as to whether or not a warrant 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 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 warrant 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.

61. 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 written authorisation signed by [Minister]. This provision intends to secure that the particulars of the case related to national security is provided to the court.

62. In order to develop safeguards for the confidentiality of the application for the interception warrant, Subsections (4) and (5) introduce a set of measures to restrict access to the application for interception warrant. 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 warrants are kept in safe custody. It is essential that such documents (including the warrants themselves) are kept confidential. The whole concept of interception as a hidden investigation could be undermined if any information concerning the applications is divulged.

63. 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 warrant 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 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 a subject of prosecution if false evidence is knowingly provided.

Section 7. Application Disclosure

64. To protect the secrecy of the investigation and to provide a safeguard for the confidentiality of the application, Section 7 criminalises the disclosure of the existence of the application for the interception warrant. 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.

65. 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 8. The Issuance of the Interception Warrant

66. The aim of this section is to provide the framework for granting an authorisation to intercept communications after applying for an interception warrant. 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] is satisfied with the necessity of carrying out interception.

67. 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] before the issuance of the interception warrant. 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] 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.

68. 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.

69. The term "national security" is not defined for the purpose of this legislative text, since it should be in line with the legislation of each national jurisdiction. It is important to avoid broad interpretation of this ground and to restrict it to particular cases which would, of course, depend on the state implementing this model legislative text.

70. Subsection (1) (a) (ii) provides the second ground for granting interception warrant: 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.

71. Subsection (1) (a) (iii) is essential to tackle the issue of mutual legal assistance in investigating serious crimes. This provision is essential as the new means of communications may entail trans-boarder 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.

72. The provision of subsection (1) (b) is essential to secure that the interception is authorised only with regard to the investigation of particular case. It is necessary to provide that a judge may authorise interception only with regard to specific crime, national security issue or mutual legal assistance request and 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.

73. The issuance of interception warrant is further restricted by the 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 interceptions is not authorised unless the information is not reasonably available by less intensive 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.

74. Subsection (1) (d) provides that an interception warrant shall be issued only if it can serve in the best interests of the administration of justice. It obliges the judge 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.

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

Section 9. Scope and Form for Interception Warrant

76. Section 9 provides rules on the scope and form of the interception warrant. 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 person and only for certain address/person/communication. A set of requirements with regard to scope and form of the interception warrant 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 the third parties.

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

78. According to the Subsection (1), an interception warrant shall be issued in the prescribed (writing) form. The writing 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, written form of the interception warrant countervails the necessity to effect particular intrusion with the need to eliminate the prospect for abuse. It is very important for an interception warrant 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.

79. Subsection (2) serves as a measure balancing the authority granted under the virtue of subsection (1). In order to strictly limit the authorisation only to 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 warrant. To comply with this provision, the interception warrant shall identify communications that should be intercepted either to or from one particular individual specified in the interception warrant or one particular address specified in the interception warrant. This is necessary to secure that interception can only be permitted for investigation of particular crime and not as a general monitoring measure.

80. 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.

81. Subsection (3) provides the possibility to include an entry clause in the interception warrant. The execution of the interception warrant 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 warrant 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 warrant.

82. 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 authorisation of entry to any premises specified in the warrant for the purpose of installing, maintaining, using or recovering any equipment used to intercept communications specified in the warrant. 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.

83. Subsection (4) requires the identification of an authorised officer on whose behalf the application is made; the person who will execute the interception warrant and the communications provider to whom the interception warrant 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 warrants as specific as possible to prevent the opportunity for abuse.

84. The model legislative text enables countries to select a person, who actually executes the interception. For countries with limited law enforcement capacity, as well as in those cases where police does not have enough resources, there is an option to define that the communication provider is obliged to intercept communication. However, the construction of Subsection (4) makes it possible for the judge to decide who will execute interception in each particular case.

85. In addition, the interception warrant 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.

86. Since the interception warrant is issued only on the basis of particular grounds, which are individual for each case, the [judge] shall be granted 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] to define ancillary provisions, conditions or restrictions relating to the interception of communications authorised in the warrant.

Section 10. Duration and Renewal of Interception Warrant

87. Section 10 is related to the duration and renewal of an interception warrant. The principal aim of this Section is to limit the authorisation to intercept to a certain period of time to avoid endless interception.

88. Furthermore, this Section provides a regulation for the renewal of the interception warrant when the period of validity established by this model legislative text and/or specified in the interception warrant turned out to be to 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.

89. The limitation of the duration of the interception warrant 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 (OESC Model Law), 3 months (Hong Kong).

90. 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 warrant shall be limited. Furthermore, the longer the duration of a warrant 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.

91. 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.

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

93. 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 warrant 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 warrant may be granted by a judge based on an application made by the Director of Public Prosecutions on behalf of an authorised officer at any time before the warrant (or any current renewal of the warrant) has expired. A country may, depending on its national legislation, allow an authorised officer to apply for a renewal without participation of Director of Public Prosecution.

94. 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 procedural for renewal should be as close to the procedures for the initial application as to keep all safeguards and prevent the risk of abuse 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 warrant. 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 warrant. 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) provides the judge with the ability to require additional information for processing the application.

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

96. According to Subsection (7) the duration of every renewal of an interception warrant may not exceed the general period of validity (as suggested by the legislative text, [90] days) and shall be specified by a judge in the renewal. A country may specify another term for the validity of the renewed interception.

97. 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 warrant is issued or a person acting on his or her behalf to apply for the revocation of the interception warrant if it appears that an interception warrant is no longer necessary.

Section 11: Modification of Interception Warrant

98. Section 11 enables an authorised officer to apply for modification of an existing interception warrant 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 warrant, changes. The process of application remains the same to secure that all safeguards are applicable. An application for modification of the existing interception warrant should be made by Director of Public Prosecutions on behalf of an authorised officer or by an authorised officer, depending on the approach that a country will choose concerning the procedure of the initial application. The grounds for the execution of the interception shall remain the same.

Section 12. Revocation of the Interception Warrant

99. This section is implemented to ensure that the interception warrant 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 model legislative text. 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’.

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

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

102. The aim of the Subsection (3) is to guarantee that if an interception warrant 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 13. Consequences of Revocation

103. This section provides a safeguard for the case of revocation of the interception warrant. Since the interception warrant is revoked if the requirements for an interception established by the legislative text are not met anymore, it is necessary to assure that the intercepted data are not used in criminal proceedings. Section 13 declares evidence that was collected while a warrant was revoked inadmissible unless the court decides that the admission of such evidence would not render the trial unfair.

Section 14. Urgent Application

104. Section 14 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.

105. 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 a warrant under such circumstances.

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

107. According to the Subsection (1) a judge may in urgent situation dispense 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 warrant. The judge shall issue the warrant if he or she is satisfied that circumstances exist that would justify the grant of an interception warrant under Section 8.

108. To ensure the formal procedure of the application, Subsection (2) establishes the requirements that any application for an emergency warrant 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 warrant; 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].

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

110. 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 warrant. 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.

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

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

113. The period of validity for every emergency interception warrant is provided by the Subsection (6) and should be [48] hours from the time it was issued. A country may choose to provide another period of the validity of the urgent interception warrant. After the period the warrant 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 warrant is transparent and finally made in written form. In addition it aims to give a judge the opportunity to review the urgent decision if there is not enough evidence for granting the interception.

114. There was a discussion within the Working Group about the procedure (written application) following the issuance of urgent interception warrant. Some Consultation Workshop participants had concerns with regard to 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 warrants, a country may choose to provide a longer period of the validity of the urgently issued warrants.

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

Section 15: Report on Progress

116. Report on progress is a necessary measure to oversight the execution of interception warrant. It enables a judge who has issued the warrant to be sure that interception is carrying in accordance with law and legal authorisation. This approach is for example used in the OESC Model Law on Interception of Communications. Section 15 gives a judge, who has issued an interception warrant, 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 considers necessary. Such order is binding and may entail the revocation of interception warrant as defined by Section 12. The request under Section 15 can be made by a judge at the time of issuance of interception warrant, or at any stage before the date of expiry.

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

Section 16: Final Report

118. This section is an option that a country 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 23.

119. 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.

120. However, a country may experience difficulties in implementing this provision as the obligation goes along with addition additional paperwork and possible privacy concerns. After an intensive discussion the Working Group agreed that countries should decide if they want to require a final report.

Section III

PART III – EXECUTION OF INTERCEPTION

121. 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 a 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 17: Execution of Interception Warrant

122. Section 16 aims to enable an authorised officer to intercept communications specified in the warrant and in accordance with its terms. In addition, it grants an authorised officer with the power to require a person that is specified in the warrant 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 warrant. 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 that is not in compliance with the interception warrant.

123. 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 warrant as well. In order to limit the intrusion of third parties' lawful interests, this subsection obliges an authorised officer or a person that intercepts or assists in the interception of communications to take all reasonable steps to minimise the impact of interception on third parties.

124. The Working Group decided to add an additional provision to the Section 17: 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 warrant. 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 18: Entry of Premise for the Execution of Interception Warrant

125. Section 18 provides the framework for the execution of the entry clause in the interception warrant, if there is one. The application of an interception warrant that contains a provision enabling the authorised officer to entry on premises shall be made in compliance with the Section 18 that permit an authorised officer to enter the premises at any time specified in the interception warrant and perform any act related to the purpose of the interception warrant.

Section 19: Duty to Provide Assistance

126. This section provides coercive measure to facilitate the interception of communications. It obliges a person, who provides communications services, to permit, and assist, if required and reasonable, an authorised officer to exercise an interception warrant. To prevent the abuse of the power to request assistance, Subsection (2) defines that the duty of a person to intercept shall be specified by a judge in the interception warrant. This provision is essential to eliminate the prospects for abuse, especially because Section 20 creates an offence on the failure to assist.

Section 20: Failure to Assist

127. Pursuant to Section 20, any person who is required to provide assistance to an authorised officer by virtue of an interception warrant and refuses to do so commits an offence. The criminalisation of the refusal to provide assistance is necessary because the interception warrant is granted in exceptional circumstances for investigation of serious crimes and the success in executing the warrant 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 21: Confidentiality of Intercepted Communications

128. 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 unauthorised use or disclosure of intercepted material.

129. Following this approach, Subsection (1) of Section 21 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 warrant with regard to the confidentiality of information, Subsection (2) specifies particular information on interception of communications and execution of interception warrant that should be kept confidential.

Section 22: Failure to Keep Information on Interception Confidential

130. Section 22 gives further protection of confidentiality of intercepted communications by establishing an offence for intentionally and without lawful excuse or justification disclosure of anything that he or she is required to keep confidential under the provisions of Section 21.

Section 23: Destruction of Records

131. 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 are 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 to keep 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.

132. In order to protect privacy, Section 23 contains an obligation to immediately destroy any records that are not related to the aim of the interception warrant. 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.

133. 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] in the final report on the execution of interception warrant. This provision is only relevant for countries that decide to include the obligation related to a final report in their interception legislation (see the explanatory note to the Section 16: Final Report).

Section 24:

134. **Failure to Destroy Records** 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 for the purpose of the interception is destroyed.

PART IV – INTERCEPTION EQUIPMENT

135. 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.

136. 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 OESC 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.

137. 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 recommendation for those countries that decide to follow the approach and create and maintain the list of the equipment with the interception capabilities.

138. The model legislative text suggests to create a 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 consultations process before the use of particular equipment is restricted or prohibited.

Section 25: Listed Equipment with Interception Capabilities

139. To secure the approach to list the equipment with interception capabilities, Section 25 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 writing 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 26. Prohibition on Manufacture, Possession and the Use of the Listed Equipment with Interception Capabilities

Section 27. Authorisation to Use the Listed Equipment with Interception Capabilities

140. To define restriction with regard to equipment that is contained in the list, Section 26 prohibits the manufacture, possession and use of listed equipment with interception capabilities unless authorised. The authorisation may be given under the Section 27 that provides a ministry with the power to grant an exemption if it is in the public interest or for 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 27 also establishes the requirements for the form and duration of certificate of exemption.

Section 28. Offence

141. In order to restrict the manufacture and possession of equipment with interception capabilities, Section 28 criminalises certain acts related to listed devices.

PART V – DISCLOSURE OF STORED COMMUNICATIONS DATA

142. Part V was developed to provide the countries with the possibility to disclose stored communication data that have already passed transmission and are therefore by definition not considered as a subject for interception.

143. 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 can not 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 OESC 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.

144. 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 and, as such, it should be made clear that this part was optional for implementation by the beneficiary states.

145. Thus, the following provisions shall be considered optional and represent recommendations for countries that may decide to follow this approach.

146. 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 the same virtue of the law as communication during their transmission. Unlawful access to stored communication data is prohibited by Section 29.

Section 29: Prohibition on Access to Stored Communication

147. 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 30: Disclosure of Stored Communications Data

148. Section 30 enables the designated person to require communication provider to obtain and/ or disclose stored communications data by using a disclosure order. As a safeguard to protect confidentiality of stored communications data, the 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 it data to an authorised officer.

149. Subsection (4) provides a set of the 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 individual case by specifying all particulars of the authorisation.

150. 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,

151. 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 31. Failure to Keep Information on the Disclosure Order Confidential

152. In order to protect the secrecy of the disclosure order, Section 31 criminalises the failure to meet confidentially requirements.

PART VI – COSTS OF INTERCEPTION

153. The allocation of cost is one of essential point of discussion 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. Furthermore, the model legislative text enables countries to set obligation to intercept communications that have to be followed by providers. Therefore, the issue of cost allocation should be solved in every jurisdiction introducing interception of communication.

Section 32: Allocation of Costs

154. This section suggests 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, a country may establish the model of reimbursement of direct costs incurred by communications provider in respect of personnel and administration required for purposes of providing assistance in execution of interception warrant.

155. 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.

156. Therefore, each country shall make its own decision regarding the approach on how to distribute costs between operators and state.

PART VII – SAFEGUARDS

157. Part VII was developed in compliance with the model policy guidelines that require to protect professional secrecy and to implement the mechanisms for monitoring and oversight with regard to the interception of communications.

158. However, concerning differences in national legislation, as well as the capacity of different countries to create monitoring and oversight bodies, the Working Group decided that this part represents a set of recommendations that country may choose to follow or not.

Section 33. Professional Secrecy

159. The model policy guidelines called for provisions protecting professional secrecy as necessary safeguards. This recommendation refers to certain types of professional communications that are subject to the obligation of professional secrecy under national laws or regulations established by competent national bodies. 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 shall not establish the privilege for communications in general as this would in the view of the members of the working group not be covered by the mandate.

160. 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 attorney-at-law is suspect of a crime that allows interception, the authorisation for interception shall be granted. However, the data gathered by such interception shall not be represented as evidence in court and shall remain privilege, if they contain professional secrecy.

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

Section 34: Monitoring of Communications Interception

162. Section 34 recommends the creation of an Independent Monitoring Authority as required by the underlying model policy guidelines. The possibility for independent monitoring of interception is necessary to strengthen the system of checks and balances with regard to such intrusive measure as interception.

163. As an option, a country may vest any authority that is not actively involved in the investigation process and has the capacity to perform necessary functions to supervise the interception with the functions of the Independent Monitoring Authority. This option is especially relevant for small countries that may experience a lack of resources.

164. This Section also gives recommendations with regard to the functions of an Independent Monitoring Authority. A country may specify them.

165. It was agreed during the discussion in the Working Group and at the Consultation Workshop plenary, that a country can decide to implement this recommendation or not depending on its national system and available resources.

Section 35. Independent Commissioner on Interception of Communications

166. This section provides the set of recommendation with regard to the creation of an independent oversight body (Independent Commissioner on Interception of Communication). As explained above, this Section is only a recommendation, which shall be implemented by countries only if considered necessary. Instead of creating a post of a commissioner, a country may also create a commission to balance the power to oversight interception and to prevent a situation where a single person in charge may abuse the access to information.

PART VIII – ADMISSIBILITY OF EVIDENCE

167. 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.

168. 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 assure 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

169. The Schedule represents a list of serious offences that, subject to Section 8, can justify the interception as a measure to carry out an investigation.

170. The Working Group inserted a new provision allowing a ministry to add offences or delete them from the list contained in the Schedule. Such an order shall be a subject to affirmative resolution.

171. The Working Group also agreed to the provision on regulations that enables a minister to undertake regulations to give effect to the purpose of this model legislative text. The regulation made under this section shall be a subject to affirmative resolution of Parliament.

172. 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 of the Firearms Act].
- An offence contrary to [section 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.

ANNEXES

Annex 1

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

Officially Designated Participants and Observers

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

Annex 1

Country	Organization	Last Name	First Name
Suriname	Telecommunicatie Autoriteit Suriname/ Telecommunication Authority Suriname	LETER	Meredith
Suriname	Ministry of Justice and Police, Department of Legislation	SITALDIN	Randhir
Trinidad and Tobago	Ministry of Public Administration, Legal Services Division	MAHARAJ	Vashti
Trinidad and Tobago	Telecommunications Authority of Trinidad and Tobago	PHILIP	Corinne
Trinidad and Tobago	Ministry of Public Administration, ICT Secretariat	SWIFT	Kevon

Regional/International Organizations' Participants

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

HIPCAR Consultants Participating in the Workshop

Last Name	First Name
MARTÍNS DE ALMEIDA	Gilberto
GERCKE	Marco
MORGAN[16]	J Paul
PRESCOD	Kwesi

[16] Workshop Chairperson

Annex 2

Participants of the Second Consultation Workshop (Stage B) for HIPCAR Project Working Group dealing with ICT Legislative Framework – Information Society Issues Crane, St. Philip, Barbados, 23-26 August 2010

Officially Designated Participants and Observers

Country	Organization	Last Name	First Name
Antigua and Barbuda	Ministry of Information, Broadcasting, Telecommunications, Science & Technology	SAMUEL	Clement
Bahamas	Utilities Regulation and Competition Authority	DORSETT	Donavon
Barbados	Ministry of Economic Affairs, Empowerment, Innovation, Trade	NICHOLLS	Anthony
Barbados	Ministry of Finance, Investment, Telecommunications and Energy	BOURNE	Reginald
Barbados	Ministry of the Civil Service	STRAUGHN	Haseley
Barbados	University of the West Indies	GITTENS	Curtis
Belize	Public Utilities Commission	PEYREFITTE	Michael
Dominica	Government of Dominica	ADRIEN-ROBERTS	Wynante
Dominica	Ministry of Information, Telecommunications and Constituency Empowerment	CADETTE	Sylvester
Dominica	Ministry of Tourism and Legal Affairs	RICHARDS-XAVIER	Pearl
Grenada	National Telecommunications Regulatory Commission	FERGUSON	Ruggles
Guyana	Office of the President	RAGHUBIR	Gita
Guyana	Public Utilities Commission	PERSAUD	Vidiahar
Jamaica	Attorney General's Chambers	SOLTAU-ROBINSON	Stacey-Ann
Jamaica	Digicel Group	GORTON	Andrew
Jamaica	LIME	SUTHERLAND CAMPBELL	Melesia
Jamaica	Ministry of National Security	BEAUMONT	Mitsy
Jamaica	Office of the Prime Minister	MURRAY	Wahkeen
Saint Kitts and Nevis	Attorney General's Chambers	POWELL WILLIAMS	Tashna
Saint Kitts and Nevis	Department of Technology, National ICT Centre	HERBERT	Christopher
Saint Kitts and Nevis	Ministry of Youth Empowerment, Sports, Information Technology, Telecommunications and Post	WHARTON	Wesley
Saint Lucia	Attorney General's Chambers	VIDAL-JULES	Gillian
Saint Lucia	Ministry of Communications, Works, Transport & Public Utilities	FELICIEN	Barrymore
Saint Vincent and the Grenadines	Ministry of Telecommunication, Science, Technology and Industry	ALEXANDER	Kelroy Andre

Annex 2

Country	Organization	Last Name	First Name
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	FRASER	Suenel
Suriname	Ministry of Trade and Industry	SAN A JONG	Imro
Suriname	Ministry of Transport, Communication and Tourism	STARKE	Cynthia
Suriname	Telecommunicatie Autoriteit Suriname/Telecommunication Authority Suriname	PELSWIJK	Wilgo
Suriname	Telecommunicatiebedrijf Suriname/Telesur	JEFFREY	Joan
Trinidad and Tobago	Ministry of National Security	GOMEZ	Marissa
Trinidad and Tobago	Ministry of Public Administration, ICT Secretariat	SWIFT	Kevon
Trinidad and Tobago	Ministry of Public Administration, Legal Services Division	MAHARAJ	Vashti
Trinidad and Tobago	Ministry of the Attorney General, Attorney General's Chambers	EVERSLEY	Ida
Trinidad and Tobago	Telecommunications Authority of Trinidad and Tobago	PERSAUD	Karina
Trinidad and Tobago	Telecommunications Services of Trinidad and Tobago Limited	BUNSEE	Frank

Regional/International Organizations' Participants

Organization	Last Name	First Name
Caribbean Centre for Development Administration (CARICAD)	GRIFFITH	Andre
Caribbean Community Secretariat (CARICOM)	JOSEPH	Simone
Caribbean ICT Virtual Community (CIVIC)	HOPE	Hallam
Caribbean ICT Virtual Community (CIVIC)	ONU	Telojo
Caribbean Telecommunications Union (CTU)	WILSON	Selby
Eastern Caribbean Telecommunications Authority (ECTEL)	WRIGHT	Ro Ann
International Telecommunication Union (ITU)	CROSS	Philip
International Telecommunication Union (ITU)	LUDWIG	Kerstin
Organization of Eastern Caribbean States Secretariat (OECS)	FRANCIS	Karlene

HIPCAR Consultants Participating in the Workshop

Last Name	First Name
ALMEIDA	Gilberto Martíns de
GERCKE	Marco
MORGAN[17]	J Paul
PRESCOD	Kwesi

[17] Workshop Chairperson.

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

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

Geneva, 2013