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

Cybercrime/e-Crimes:

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

Cybercrime/e-Crimes:

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 than 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 Dr. Marco Gercke and Ms. Pricilla Banner. 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 Saint Kitts and Nevis on 19 – 22 July 2010 (see Annexes). The explanatory notes to the model legislative text in this document were prepared by Dr. Marco 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. The team at ITU's Publication Composition Service was responsible for its publication.

Table of contents

Page

Introduction

1.1. HIPCAR Project – Aims and Beneficiaries

The HIPCAR project[1] was launched by the International Telecommunication Union (ITU) and the European Union (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, Saint Kitts and Nevis, Saint Lucia, Saint 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).

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

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

[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.

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, Saint Lucia, Saint 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.

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 Cybercrime, 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 Cybercrime 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 HIPCAR Steering Committee – chaired by the Caribbean Telecommunications Union (CTU) – provided guidance and support to a team of consultants, including Dr. Marco Gercke and Ms. Pricilla Banner. The model legislative text on Cybercrime was developed in three phases initially by HIPCAR consultants: (1) the drafting of an assessment report; (2) the development of model policy guidelines; and (3) the drafting of the model legislative text. The draft documents were then reviewed, discussed and adopted by broad consensus by participants at two consultation workshops for the HIPCAR Working Group on Information

[3] See HIPCAR "Cybercrime: Assessment Report" available at www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/

Society Issues, held in Saint Lucia on 8-12 March 2010 and in Saint Kitts and Nevis on 19-22 July 2010 (see Annexes). The explanatory notes to the model legislative text in this document were prepared by Dr. Marco Gercke addressing, *inter alia*, the points raised at the second workshop. This document therefore contains data and information as known in July 2010.

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 Fighting Cybercrime

In the last decades, computer crime and Cybercrime have become a major concern for law enforcement around the world. Since the debate about criminal abuse of computer and network technology started in the 1960s, the importance of the topic has constantly emerged.[4] During half of a century of intensive debate, various solutions have been discussed to address the issue. However, especially due to constant technical developments as well as the changing methods as to how the offences are carried out, the issue remains on the agenda of both national governments and international/regional organisations.

From the 1960s to the 1980s, computer manipulation and data espionage – often not covered by existing criminal legislation – and especially the development of a legal response, constituted the focus of the debate.[5] This changed in the 1990s when graphical interface ("WWW") was introduced and the number of websites and internet users started to grow dramatically. It then became possible to make information legally available in one country and enable users anywhere in the world to download it – even in those countries where the publication of such information was criminalised.[6]

In the last few years, the debate has been dominated by new, very sophisticated methods of committing crimes such as "Phishing[7]", "Botnet[8] Attacks" and the emerging use of technologies that are more difficult for law enforcement to investigate, such as "Voice-over-IP (VoIP) communication"[9] and "Cloud Computing"[10].

The ability to fight Cybercrime is essential for both developed and developing countries. With a growing dependence on the availability of networks and computer systems[11] as well as the growing number of Internet users, crimes committed by using information technology will most likely become more frequent and potentially more severe. In order to protect users that have started to integrate network services such as e-mail, communication through social networks and electronic banking, countries must have the

4 Regarding the early discussion about computer crime see: *Bequai*, Computer Crime, 1978; *Blanton*, Computer Crime, 1978; *Coughran*, Computer abuse and criminal law, 1976; *MacIntyre*, Computer and Crime, 1977; *McKnight*, Computer Crime, 1973; *Parker*, Crime by Computer, 1976; *Rose*, An analysis of computer related crime: A research study, 1977; *Sokolik*, Computer Crime: Its setting and the need for deterrent legislation, 1979; *Wilson/Leibholz*, User's Guide to Computer Crime: Its Commission, Detection and Prevention, 1969.

5 See for example: *Nycum*, The criminal law aspects of computer abuse: Applicability of federal criminal code to computer abuse, 1976; *Sieber*, Computerkriminalitaet und Strafrecht, 1977.

6 Regarding the transnational dimension of cybercrime see: *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 7.

7 The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. For more information see: Understanding Cybercrime: A Guide for Developing Countries, ITU 2009, Chapter 2.8.4.

8 Botnets is a short term for a group of compromised computers running a software that are under external control. For more details, see *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4.

9 *Simon/Slay*, "Voice over IP: Forensic Computing Implications", 2006.

10 *Velasco San Martin,* Jurisdictional Aspects of Cloud Computing, 2009; *Gercke*, Impact of Cloud Computing on Cybercrime Investigation, published in Taeger/Wiebe, Inside the Cloud, 2009, page 499 et seq.

11 See in this regard: Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009, page 65.

ability to act when those services are attacked or abused in other ways. But the importance of having the ability to carry out investigations in order to identify offenders and collect digital evidence goes beyond consumer protection. The Internet is a global market place and companies can offer services worldwide. If countries want to create an environment that allows e-commerce to grow, in the long term they need to ensure that crimes against such businesses do not go unpunished.

As a consequence, dealing with Cybercrime has made it to the top of the agenda in most countries. It is important to underline that – unlike other topics – it is most likely that this topic will remain a priority for years given that addressing the issue is not something that can be done only once and forever. Cybercrime is constantly developing, and legal solutions will need continued adjustments from time to time.

Reducing the response to technical solutions will most likely not solve the problems. Some of the technical solutions being implemented as part of anti-cybercrime strategies often include firewalls (preventing illegal access to computer systems) or encryption (to prevent illegal interception of communications). But past experience has shown that – in addition to technical solutions – legislative measures are also needed: an efficient penal legislation criminalising certain forms of computer crime and cybercrime as well as the existence of related procedural instruments that enable law enforcement to carry out investigations are essential requirements for the involvement of law-enforcement agencies in the fight against computer crime and cybercrime. Those countries that do not have adequate legislation in place risk, first of all, that law enforcement agencies will not be able to support citizens that have become victims of computer crimes. But even more serious is the fact that the absence of criminalisation of certain cybercrimes might protect offenders or even motivate them to move illegal activities from abroad to countries with missing legislation. Preventing "safe havens" from where criminals are able to operate with impunity has therefore become a key challenge in preventing cybercrime.[12] Wherever "safe havens" do exist, there is a threat that offenders will use them to evade investigation. One well-known example of this is the "Love Bug" computer worm, developed by a suspect in the Philippines in 2000,[13] which infected millions of computers worldwide.[14] Local investigations were hindered by the fact that the development and spreading of malicious software was not at that time adequately criminalised in the Philippines.[15]

12 This issue was addressed by a number of international organisations. The UN General Assembly Resolution 55/63 points out: "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies". The full text of the Resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: "There must be no safe havens for those who abuse information technologies". See below: Understanding Cybercrime: A Guide for Developing Countries, ITU 2009, Chapter 5.2.

13 For more information, see http://en.wikipedia.org/wiki/ILOVEYOU; regarding the effect of the worm on Critical Information Infrastructure Protection, see: *Brock*, "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities, 2000.

14 BBC News, "Police close in on Love Bug culprit", 06.05.2000.

15 See for example: CNN, "Love Bug virus raises spectre of cyberterrorism", 08.05.2000; *Chawki*, "A Critical Look at the Regulation of Cybercrime", www.crime-research.org/articles/Critical/2; *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 10; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233.

Introduction

Although the development of new technologies is focused mainly on meeting consumer demands in western countries, developing countries have – despite the remaining need for further enhancement – undertaken significant progress in narrowing the gap, especially with regard to access to information.[16] In 2005, the number of Internet users in developing countries surpassed the number in the industrialised nations.[17] With the growing connectivity and the transformation of traditional business into e-commerce, cybercrime is no longer an issue only for developed, but also for developing countries.[18] However, developing countries in general – and small island countries in particular – face a number of specific challenges while implementing legislation. While the crimes that they are facing are up to a certain extent the same as those that developed countries are confronted with, developing countries have special demands when it comes to the response. Developed countries might, for example, be able to afford a so-called 24/7 network point for international mutual legal assistance requests. Developing countries often do not have the capacity to maintain such infrastructure. It is therefore essential that developing countries take into consideration international standards as well as their specific situation when developing an anti-cybercrime strategy in general and Cybercrime legislation in particular.

16 Regarding the possibilities and technology available to access the Internet in developing countries, see: *Esteve/Machin*, Devices to access Internet in Developing countries, available at: www2007.org/workshops/paper_106.pdf.

17 See "Development Gateway's Special Report, Information Society – Next Steps?", 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

18 The specific demands of developing countries are addressed in the ITU publication "Understanding Cybercrime: A Guide for Developing Countries" that was published in 2009 and is made available free of charge in all six UN languages.

Section I:
Model Policy Guidelines – Cybercrime/e-Crimes

Following, are the Model Policy Guidelines that a country may wish to consider in relation to Cybercrime/e-Crimes.

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

- There shall be proper definition on “computer”, “computer system”, “device”, “computer data”, “content data”, “traffic data”, “location data”, “document”, “electronic record”, “electronic document”, “electronic signature”, “digital signature”, and “time-stamping”.
- There shall be sufficiently broad wording in the definition of these terms, coupled with a list of illustrative examples.
- There shall be definition on what terminology shall be left for judicial construction, and on how to follow-on on such judicial activity to keep statutory definitions and judicial definitions aligned – at the national level, each member state will decide which option is best for them.
- Facilitate harmonization through the sharing of judicial precedents: define specific technical terms as far as possible.
- Training material shall be developed to provide investigators, prosecutors and judges with the necessary interpretation of those terms if required including relevant stakeholders.

Section I

2. CARICOM/CARIFORUM COUNTRIES SHALL DEVELOP SUBSTANTIVE CRIMINAL LAW DEALING WITH CYBERCRIME

- There shall be provisions covering the most common and internationally widely accepted forms of Cybercrime as well as those offences that are of specific interest for the region (such as for example SPAM).
- To ensure the ability to cooperate with law enforcement agencies from countries in the region as well as outside the region the legislation shall be compatible to both international standards and best practices as well as (up to the largest extent possible) to existing regional standards and best practices.
- There shall be a provision criminalizing the intentional and illegal access to a computer system as well as illegally remaining in a computer system. An aggravation of penalty in cases where protection measures were circumvented to intercept the transmission could be taken into consideration.
- There shall be a provision criminalizing the intentional and illegal interception of non-public data transmission (illegal interception). This provision should not hinder a lawful interception by competent authorities. An aggravation of penalty in cases where protection measures were circumvented to intercept the transmission could be taken into consideration.
- There shall be a provision criminalizing intentional and illegal interference with computer data. It should be ensured that the application of procedural instrument necessary for investigations is not hindered in cases where the offender commits several offences and each only leads to limited damage.
- There shall be a provision criminalizing intentional and illegal interference with computer systems (such as denial of service attacks). An aggravation of penalty in cases where critical infrastructure is affected could be taken into consideration.
- There shall be a provision criminalizing intentional and illegal production, sale and related acts of tools that are primarily designed to commit computer crimes. It should be ensured that such legislation does not criminalize the legitimate use of such software tools.
- There shall be a provision criminalizing intentional and illegal computer-related forgery. It should be ensured that such legislation especially covers acts of sending out phishing emails. An aggravation of penalty in cases where numerous emails are sent out should be taken into consideration.
- There shall be a provision criminalizing intentional and illegal computer-related fraud.
- It should be ensured that existing legislation criminalizing fraud is also applicable if offenders are using means of electronic communication to communicate with the victim.
- There should be a provision criminalizing the intentional and illegal production, sale and related acts related to child pornography. Especially in this respect international standards should be taken into consideration. The legislation should in addition cover the criminalization of the possession of child pornography and gaining access to child pornography websites. An exemption that enables law enforcement agencies to carry out investigations should be included.
- There should be a provision criminalizing acts related to sending out SPAM if it affects the ability of users to make use of Internet access.[19]
- The legislation should reflect the challenges related to attribution.
- There should be a provision criminalizing intentional and illegal acts of identity-related crime. The different phases of identity theft (obtaining, transferring and using identity-related information) should be taken into consideration

[19] (There remains a concern about the proportionality of the remedy)

3. CARICOM/CARIFORUM COUNTRIES SHALL DEVELOP EFFECTIVE BUT BALANCED PROCEDURAL INSTRUMENTS THAT ENABLE COMPETENT AUTHORITIES TO INVESTIGATE CYBERCRIME BUT PROTECT THE RIGHTS OF THE SUSPECT.

- The procedural instruments should not interfere with the internationally as well as regionally accepted fundamental rights of the suspect.
- There should be a provision enabling competent authorities to order the expedited preservation of computer data.
- There should be a provision enabling competent authorities to order the partial disclosure of preserved computer data.
- There should be a provision enabling competent authorities to order the production of computer data.
- There should be a provision enabling competent authorities to use specific search and seizure instruments related to digital evidence and computer technology. The law shall regulate search and seizure proceedings in a way to avoid the collection of evidence being questioned as not having been certified and produced as material evidence of the data collected and of the existing digital environment.
- There should be a provision enabling competent authorities to order the lawful collection of traffic data and the lawful interception of content data.
- Limited to cases of serious crime there should be a provision enabling competent authorities to make use of sophisticated investigation instruments such as the use of key-loggers and remote forensic software to collect passwords used by a suspect of such crime or identify the connection used by a suspect.

4. CARICOM/CARIFORUM COUNTRIES SHALL DEVELOP INSTRUMENTS FOR TRANSNATIONAL COOPERATION IN CYBERCRIME INVESTIGATIONS

- The framework for international cooperation should reflect international standards of cooperation as well as the specific needs with regard to Cybercrime investigation.
- The framework should include the creation of a designated 24/7 point of contact for requests.
- The framework should enable the use of expedited means of communication (such as email and fax).

5. CARICOM/CARIFORUM COUNTRIES SHALL DEVELOP A FRAMEWORK REGULATING THE RESPONSIBILITY OF INTERNET SERVICE PROVIDERS

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

Section II: Model Legislative Text – Cybercrime/e-Crimes

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

Arrangement of Sections

Section II

Section II

PART I – PRELIMINARY

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

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

Definitions 3. (1) Access provider means any natural or legal person providing an electronic data transmission service by transmitting information provided by or to a user of the service in a communication network or providing access to a communication network.

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

(3) Child shall mean any person under the age of eighteen (18) years.

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

a. a child engaged in sexually explicit conduct;

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

c. images representing a child engaged in sexually explicit conduct;

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

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

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

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

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

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

(9) Device includes but is not limited to

a. components of computer systems such as graphic cards, memory, chips;

b. storage components such as hard drives, memory cards, compact discs, tapes;

c. input devices such as keyboards, mouse, track pad, scanner, digital cameras;

d. output devices such as printer, screens.

(10) Hinder in relation to a computer system includes but is not limited to:

a. cutting the electricity supply to a computer system; and

b. causing electromagnetic interference to a computer system; and

c. corrupting a computer system by any means; and

d. inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

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

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

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

(14) Multiple electronic mail messages mean a mail message including E-Mail and instant messaging sent to more that thousand recipients.

(15) Remote forensic software means investigative software installed on a computer system and used to perform tasks that include but are not limited to keystroke logging or transmission of an IP-address.

(16) Seize includes:

a. activating any onsite computer system and computer data storage media;

b. making and retaining a copy of computer data, including by using onsite equipment;

c. maintaining the integrity of the relevant stored computer data;

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

e. taking a printout of output of computer data; or

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

(17) Internet service provider means a natural or legal person that provides to users services mentioned in sections 28 – 33 hereof.

(18) Traffic data means computer data that:

a. relates to a communication by means of a computer system; and

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

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

(19) Thing includes but not limited to:

a. a computer system or part of a computer system;

b. another computer system, if:

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

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

c. a computer data storage medium.

(20) Utilise shall include

a. developing of a remote forensic software; and

b. adopting of a remote forensic software; and

c. purchasing of a remote forensic software.

PART II – OFFENCES

Illegal Access

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

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

Illegal Remaining

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

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

Illegal Interception

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

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

   b. electromagnetic emissions from a computer system

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

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

Illegal Data Interference

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

a. damages or deteriorates computer data; or

b. deletes computer data ; or

c. alters computer data; or

d. renders computer data meaningless, useless or ineffective; or

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

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

g. denies access to computer data to any person authorized to access it;

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

Data Espionage

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

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

Illegal System Interference

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

a. hinders or interferes with the functioning of a computer system; or

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

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

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

Illegal Devices

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

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

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

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

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

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

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

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

Computer-related Forgery

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

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

Computer-related Fraud

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

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

b. any interference with the functioning of a computer system,

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

Child Pornography

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

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

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

c. distributes or transmits child pornography through a computer system;

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

e. Possesses child pornography in a computer system or on a computer-data storage medium; or

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

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

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

(3) A country may not criminalize the conduct described in section 13 (1) (d)-(f).

Identity-related Crimes

14. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification by using a computer system in any stage of the offence, intentionally transfers, possesses, or uses, without lawful excuse or justification, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a crime, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

SPAM

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

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

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

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

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

(2) A country may restrict the criminalization with regard to the transmission of multiple electronic messages within customer or business relationships. A country may decide not to criminalize the conduct in section 15 (1) (a) provided that other effective remedies are available.

Disclosure of Details of an Investigation

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

a. the fact that an order has been made; or

b. anything done under the order; or

c. any data collected or recorded under the order;

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

Failure to Permit Assistance

17. (1) A person other than the suspect who intentionally fails without lawful excuse or justification or in excess of a lawful excuse or justification to permit or assist a person based on an order as specified by sections 20 to 22 commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

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

Harassment Utilizing Means of Electronic Communica-tion

18. A person, who without lawful excuse or justification or in excess of a lawful excuse or justification initiates any electronic communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, using a computer system to support severe, repeated, and hostile behavior, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

PART III – JURISDICTION

Jurisdiction

19. This Act applies to an act done or an omission made:

a. in the territory of [enacting country]; or

b. on a ship or aircraft registered in [enacting country]; or

c. by a national of [enacting country] outside the jurisdiction of any country; or

by a national of [enacting country] outside the territory of [enacting country], if the person's conduct would also constitute an offence under a law of the country where the offence was committed.

PART IV – PROCEDURAL LAW

Search and Seizure

20. (1) If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds [to suspect] [to believe] that there may be in a place a thing or computer data:

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

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

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

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

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

(2) If [law enforcement] [police] officer that is undertaking a search based on Sec. 20 (1) has grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, he shall be able to expeditiously extend the search or similar accessing to the other system.

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

Assistance

21. Any person who is not a suspect of a crime but who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein that is the subject of a search under section 20 must permit, and assist if reasonably required and requested by the person authorized to make the search by:

a. providing information that enables the undertaking of measures referred to in section 20;

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

c. obtaining and copying such computer data;

d. using equipment to make copies; and

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

Production Order

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

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

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

Expedited Preservation

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

Partial Disclosure of Traffic Data

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

a. the Internet service providers; and/or

b. the path through which the communication was transmitted.

Collection of Traffic Data

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

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

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

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

(3) A country may decide not to implement section 25.

Interception of Content Data

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

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

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

(2) A country may decide not to implement section 26.

Forensic Software

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

a. suspect of the offence, if possible with name and address; and

b. description of the targeted computer system; and

c. description of the intended measure, extent and duration of the utilization; and

d. reasons for the necessity of the utilization.

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

a. the technical mean used and time and date of the application; and

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

c. any information obtained.

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

(3) The duration of authorization in section 27 (1) is limited to [3 months]. If the conditions of the authorization is no longer met, the action taken are to stop immediately.

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

(5) If the installation process requires physical access to a place the requirements of section 20 need to be fulfilled.

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

(7) [List of offences].

(8) A country may decide not to implement section 27.

PART V – LIABILITY

No Monitoring Obligation

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

Access Provider

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

a. does not initiate the transmission;

b. does not select the receiver of the transmission; or

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

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

Hosting Provider

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

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

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

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

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

Caching Provider

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

a. the caching provider does not modify the information;

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

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

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

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

Hyperlinks Provider

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

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

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

Search Engine Provider

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

a. does not initiate the transmission; and

b. does not select the receiver of the transmission; and

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

Section III:
Explanatory Notes to Model Legislative Text on Cybercrime/e-Crimes

INTRODUCTION

1. This legislative text provides a legal framework for the criminalisation of computer and network related offences. The principal aims of this model legislative text are to criminalize certain illegal content in line with regional and international best practices, provide the necessary specific procedural instruments for the investigation of such offences and define the liability of service provider.

2. These explanatory notes are prepared to explain the content of the model legislative text, and need to be read in conjunction with it. They explain the importance of the provisions and, where applicable, reflect the discussions within the HIPCAR[20] Working Group[21]. They are not, and are not meant to be, a detailed description of this legislative text. 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, no detailed explanation is given.

3. The model legislative text (Act) consists of five parts:

   - **Part I** provides definitions and sets the objective of the Act;
   - **Part II** provides a set of substantive criminal law provisions that criminalise certain offences;
   - **Part III** provides procedures to determine jurisdiction;
   - **Part IV** provides a set of procedural instruments necessary to investigate Cybercrime;
   - **Part V** defines limitations of the liability of Internet service providers.

[20] 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).

[21] 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 related to Cybercrime was held in St. Kitts and Nevis, 19 – 22 July 2010. Participants reviewed, discussed and adopted the Draft Model Legislative Text on the respective area of work. Where ever the words "working group" or "drafters" appear in this document, it refers to the aforementioned Workshop.

COMMENTARY ON SECTIONS

PART I

Section 1. Definitions

(1) Access Provider

The drafters of the legislative text decided to limit the responsibility of certain Internet Service Providers if their ability to prevent users from committing crimes is limited. It was therefore necessary to differentiate between the different types of provider. Sec. 3 (1) underlines that the term "access provider" can be both a legal person as well as a natural person. In light of this, even the operator of a private network can therefore be considered an access provider.

(2) Caching Provider

Caching of content is a widely used technique to enhance the speed of access to popular information. It especially covers the storage of popular websites by service providers on local storage media in order to reduce the bandwidth and make access to data more efficient. This can for example be undertaken by setting up proxy servers. The process of copying data only leads to a qualification as caching provider if the provider configures its systems in a way that the storage process is undertaken automatically, intermediately and temporarily for the sole purpose of enhancing the efficiency of onward transmission. Manual storage as well as long-term storage are therefore not covered.

(3) Child

The term child was defined in accordance with Article 1 of the UN Convention of the Rights of the Child. Details of the determination of age, for example the question of the appearance can be used in cases where information about the real age of the child cannot be obtained, are left to the national lawmakers to determine in accordance with the requirements of their domestic laws. Definition (7) in this respect contains certain guidance with regard to child pornography.

(4) Child Pornography

The definition of child pornography was intensively discussed by the drafters of the legislative text. While there was a wide agreement that child pornography should cover the documentation of a real abuse, the drafters decided to leave it to the national law-maker to determine if whether they also want to cover persons only appearing to be a child or images representing a minor. In this context the drafters took into account that in contemporary circumstances realistic images can be easily created by using sophisticated computer technology and that such pictures can be used to encourage or seduce children to participate in such acts.

With regard to the fact that child pornography is not only distributed as pictures and video the drafters decided to choose language that enables the coverage of audio, visual or text material.

(5) Computer System

Computer system and information system are both terms used to describe data processing devices that in general combine hardware and software. Computer systems therefore include input, output, and storage facilities as long as they contain data processing components. The drafters of the legislative text decided to extent the definition to also include the Internet.

(6) Computer Data

The drafters decided to base the definition of computer data on international standards. In order to ensure that all types of content are covered the drafters provided examples in brackets.

(7) Computer Data Storage Medium

Not only the capacity but also the size and function of computer storage devices have changed within the last decades. The drafters decided to formulate an open definition that covers mass storage devices as well as micro storage systems that are for example used in car keys. This provision is therefore applicable to both permanent as well as short-term storage devices (such as RAM).

(8) Critical Infrastructure

Today computer systems are not only used by private persons and businesses but also by the operators of critical infrastructure, such as energy supply or traffic control. As infrastructure that is considered critical varies from country to country the drafters decided to include a broad definition of critical infrastructure.

(9) Devices

The drafters decided to provide an open ended approach to the application of provisions referring to a device by providing a set of examples. This list of examples is therefore not conclusive or limited but open for new developments.

(10) Hinder

Some of the international approaches to address Cybercrime criminalize the illegal hindering of computer systems without providing a precise definition of what is covered by the Act. The drafters decided to ensure that the term hindering includes network based attacks (such as the transmission of computer data) as well as physical attacks. Accidental cuts of power supply are covered by definition but are excluded from criminal liability as the related provision (Sec. 9) requires the commission of the act as well as intent.

(11) Hosting Provider

Similar to the definition of other categories of Internet service providers, the term hosting provider not only includes a legal person but also a natural person. It is not necessary that the hosting provider possesses storage devices. The operator of a website that allows users to post messages also acts as a hosting provider.

(12) Hyperlink

The drafters decide to regulate the criminal responsibility of a hyperlink provider. In this context the law provides a broad definition of hyperlink to cover the various different technical solutions.

(13) Interception

The interception of data transfer processes is a procedural instrument that can be found in different international approaches to address Cybercrime. However, most of these instruments do not specify the acts or provide details of the legitimate investigation procedures. The drafters decided to include some examples for both legitimate acts as well as the types of communication that can be interception.

(14) Multiple Electronic Mail Messages

The drafters recognised the potential negative impact of SPAM for developing countries. One essential component of a criminalisation of SPAM is the definition of multiple messages. In light of this the drafters decided to require at least one thousand (1,000) messages.

(15) Remote Forensic Software

One of the aspects that was intensively discussed during the negotiation of the legislative text was the conduct of sophisticated investigation procedures. The drafters took note of reports about the use of remote forensic software in national investigations. With regard to the definition of remote forensic software they decided to highlight the possible fields where such software could be used (keystroke logging and transmission of IP-addresses) but not limit the scope of such software to these functions.

(16) Seize

The seizure of evidence is a traditional investigation process. Taking into account that in addition to the seizure of hardware there are various ways in which evidence can be collected. The drafters decided to further elaborate on this definition by providing examples of activities that are considered to be part of the seizure of evidence. One example that was included in the definition is the authorization to activate the suspect's computer system. The drafters found it worth mentioning that this is an essential requirement for sophisticated investigations.

(17) Internet Service Provider

In lieu of providing a single definition of Internet Service Provider the drafters decide to differentiate between the types of service providers.

(18) Traffic Data

The interception of traffic data is an important investigation process. The drafters decided to provide a set of criteria that clearly define and thereby limit the applicability of the provision to the relevant categories of data.

(19) Things

Things are object of seizure. While the interpretation of the term is left to national courts the drafters decided to provide a set of examples.

(20) Utilise

The definition of the term "utilise" is relevant for the use of remote forensic software. As a result of an intensive discussion during the working group session the drafters decided to clarify that not only the use of such software, but also preparatory acts are covered by the provision.

PART II

Introduction to Sections 4 – 15

The purpose of Sections 4-15 of the Legislative Text is to improve the means to prevent and investigate computer– and network-related crime by defining a common minimum standard of relevant offences based on best practice prevailing within the region as well as international standards. In this context the definition of standards by Sections 4-15 will help national lawmakers to discover possible gaps in domestic law and also form the basis for closer international cooperation that in general requires a similar degree of criminalisation as a consequence of the double criminality requirement. Sections 4-15 provide a definition of the minimum standards and therefore do not preclude more extensive criminalisation on the national level.

During the discussion the working group decided to add certain qualifying circumstances to restrict the criminalisation that is reflective of the different assessments of the dangerous nature of the behaviour involved or of the need to use criminal law as a countermeasure within the region. This approach provides flexibility to the various states in determining their criminal policy in this area.

Section 4: Illegal Access

This provision criminalises the act of access. The protected legal interest is the integrity of the computer system. The need for criminalisation of such acts reflects the interests of operators or computer systems to run their systems in an undisturbed manner. The mere unauthorised intrusion and not only follow up crimes such as data interferences should therefore be criminalised as it my lead to impediments to legitimate users of systems and data and may generate high costs for reconstruction. The provision completes technical approaches to prevent such conduct (e.g. password protection measures) and enables law enforcement agencies to carry out investigations in such cases where offenders successfully manage to commit the offence.

Access does not specify a certain means of communication, but is open-ended and facilitates further technical developments. It shall include all means of entering another computer system, including Internet attacks, as well as illegal access to wireless networks. Even unauthorised access to computers that are not connected to any network (e.g. by circumventing a password protection) are covered by the provision. Like all other offences established in this document Section 4 requires that the offender is carrying out the offences intentionally. Reckless acts are therefore not covered.

Access to a computer system can only be prosecuted under Section 4, if it happens “without lawful excuse or justification”. This requires that the offender acts without authority (whether legislative, executive, administrative, judicial, contractual or consensual) and the conduct is otherwise not covered by established legal defences, excuses, justifications or relevant principles. Access to a system permitting free and open access by the public or access to a system with the authorisation of the owner or other rights-holder is as a consequently not criminalised. Network administrators and security companies that test the protection of computer systems in order to identify potential gaps in security measures do not commit a criminal act.

The fact, that the victim of the crime proffered a password or similar access code to the offender, eg because the offender persuaded the victim to disclose a password or access code due to a successful social engineering approach, does not necessarily mean that the offender then acted legitimately when he accessed the computer system of the victim.

Section 5: Illegal Remaining

This provision criminalises the illegal remaining in a computer system. Similar to Section 4 the protected legal interest is the integrity of the computer system. The provision, that is in similar form neither contained in the Commonwealth Model Law nor Council of Europe Convention on Cybercrime is reflecting the fact, that the integrity of a computer system can not only be violated by entering a computer system without right but also by remaining in the computer system after the authorisation has expired. Such conduct cannot be covered by Section 4 as in such cases the offender did not illegally enter the system.

Remaining requires that the offender still has access to the computer system. This can for example be the case if the offender remains logged on or continues to undertake operations. The fact that he has the theoretical possibility to log on to the computer system is not sufficient.

Section 4 requires that the offender is carrying out the offences intentionally. Reckless acts are not covered by this section. Section 4 only criminalizes such acts that are committed “without lawful excuse or justification”.

Section 6: Illegal Interception

This provision aims to equate the protection of electronic transfers with the protection of voice conversations against illegal tapping and/or recording that currently already exists in most legal systems. The offence in general applies to all forms of electronic data transfer (e.g. telephone, fax, file transfer or e-mail).

The applicability of Section 3 is limited to the interception of transmissions realised by technical measures. Interception related to electronic data can be defined as any act of acquiring data during a transfer process. Interception related to electronic data can be defined as any act of acquiring data during a transfer process. This can be done by listening to, monitoring or surveillance of the content of communications. This provision only applies to the interception of transmissions therefore access to stored information is not considered as an interception of a transmission.

The term "transmission" covers all data transfers, whether by telephone, fax, e-mail or file transfer. The offence established under Section 6 applies only to non-public transmissions. A transmission is "non-public", if the transmission process is confidential. The vital element to differentiate between public and non-public transmissions is not the nature of the data transmitted, but the nature of the transmission process itself. Even the interception of publicly available information can be considered criminal, if the parties involved in the transfer intend to keep the content of their communications secret. Use of public networks does not exclude "non-public" communications.

The inclusion of electromagnetic emissions within the legislative text ensures that a comprehensive approach is undertaken, especially as older computers generate electromagnetic emissions during their operation. Such emissions that are not covered by the term data within the legislative text needed to be specifically criminalised.

Section6 requires that the offender carries out or perpetrates the offences intentionally and without lawful excuse or justification. This is not the case if the interception takes place on the basis of instructions or with the authorisation of the participants of the transmission or it is a lawful interception on the basis of criminal law provisions.

Section 7: Illegal Data Interference

Section 7 aims to fill existing gaps in some national criminal laws as well as provide computer data and computer programmes with protections similar to those enjoyed by tangible objects against the intentional infliction of damage.

The terms damaging and deterioration mean any act related to the negative alteration of the integrity of data and software. To a certain degree these terms contain an essential overlap. "Deleting" covers such acts where information is removed from storage media and is considered comparable to the destruction of a tangible object. Dropping a file to the virtual trash bin does not remove the file from the hard disk and is therefore not considered an act of deletion but can be covered by the term denial of access. Altering data covers the modification of existing data, without necessarily lowering the serviceability of the data. This act is especially covering the installation of malicious software like spyware, viruses or adware on the victim's computer even if they do not operate afterwards.

The term "Rendering meaningless" covers all acts of interference with data that makes it unprocessable with regard to its intended use. This act requires that the data was useful or effective before such interference.

"Obstructing, interrupting and interfering with the lawful use or any person in the lawful use" covers any action that negatively influences a lawful data processing process. The application of the provision is especially discussed with regard to Denial-of-Service attacks. During the attack the data provided on the

targeted computer system no longer becomes available for potential lawful users as well as the owner of the computer system. However a more specific provision (Section 9) was included to ensure the criminalisation of such acts.

The suppression of computer data denotes an action that affects the availability of data to the person with access to the medium, where the information is stored in a negative way.

Section 6 requires that the offender carries out the offences intentionally and without lawful excuse or justification. The right to alter data was discussed, especially in the context of "remailers" that are used to modify certain data for the purpose of facilitating anonymous communications. The intentional use of such services is considered an authorisation for the necessary alterations.

Section 8: Data Espionage

The Convention on Cybercrime as well as the Commonwealth Model Law and the Stanford Draft Convention provide legal solutions for illegal interception, but not for illegally obtaining data. It is questionable whether Article 3 of the Convention on Cybercrime applies to other cases than those where offences are carried out by intercepting data transfer processes.

Section 8 protects the secrecy of stored and protected computer data. Unlike other approaches this section not only covers economic secrets, but also stored computer data in general. In terms of its objects of protection, this approach is broad in nature, but the application of the provision is limited as obtaining data is only criminalised where data are specially protected against unauthorised access. The special protection requires that the hoster of the information has implemented protection measures that significantly increase the difficulty of obtaining access to the data without authorisation. Examples are password protection and encryption. It is necessary that the protection measures go beyond standard protection measures that apply to data as well as other property, for example access restrictions to certain parts of government buildings. On the other hand it is not necessary that the measures are computer technology related. Even physical measures like locks enable the application of the provision.

The act of obtaining covers any activity undertaken by the offender to obtain possession of the relevant data. This can for example be done by removing a storage device or copying files from the original source to the offender's storage device.

Section 9: System Interference

In order to protect access of operators and users to ICTs a provision was included that criminalizes the intentional hindering of the lawful use of a computer system. This provision therefore aims to protect the integrity of computer systems. The application of the provision requires that the offender hinders or interferes the functioning of a computer system.

"Hindering" means any act that interferes with the proper functioning of a computer system. The term is further defined in Section 3. The working group discussed whether the problem of spam e-mail could be addressed under Section 5, since spam can overload computer systems. Due to the fact that the application of a similar provision in the Convention on Cybercrime in relation to SPAM evinced challenges the drafters decided to include a specific provision that addressed SPAM in Section 15. Section 9 requires that the offender carries out the offences intentionally and without lawful excuse or justification. It therefore stands to follow that authorised computer test shall not be criminalised.

Subparagraph 2 contains a regulation pertaining to an aggravated penalty if the offences affects critical infrastructure. The functioning of computer system has become essential for the control of critical infrastructure such as health care, transportation and energy supply. Subparagraph 2 therefore takes this threat into consideration by providing the possibility to refer to higher penalties.

Two different cases are mentioned in subparagraph 2, viz. (1) affecting computer systems that are exclusively used for critical infrastructure operations and (2) affecting computer systems that do not exclusively operate critical infrastructure but are among other purposes used for critical infrastructure protection. In the latter case it is necessary to prove that the conduct did take place at a time when the computer system was operating critical infrastructure operations.

Section 10: Illegal Devices

Paragraph 1(a) identifies both the devices designed to commit and promote cybercrime as well as passwords that enable access to a computer system. The term devices covers hardware and software based solutions that are aimed at committing one of the mentioned offences. Examples of such software are virus programs, or programs designed or adapted to gain access to computer systems. Computer password, access code, or similar data are unlike devices not performing operations but access codes. Examples are published passwords that enable access to paid services and data bases. The publication of system vulnerabilities, that could serve as an instruction how to circumvent protection measures are not covered by the provision as long as they do not contain access codes. Unlike classic access codes system vulnerabilities it does not necessarily enable immediate access to a computer system but enables the offender to make use of the vulnerabilities to successfully attack a computer system.

“Production” means any process of creating either a device or password. The production of non-executable parts of software shall not be covered. “Sale” describes the activities involved in selling the devices and passwords in return for money or other compensation. “Procurement for use” covers acts related to the active obtaining of passwords and devices. The fact that the act of procuring is linked to the use of such tools in general requires intent of the offender to procure the tools with the objective of using it in a manner that goes beyond “regular” intent and “that it be used for the purpose of committing any of the offences established by part II.

“Import” relates to acts of obtaining devices and access codes from foreign countries. As a result, offenders that import such tools for the purpose of selling them can be prosecuted even before they offer the tools for sale. With regard to the fact, that the procurement of such tools is only criminalised if it can be linked to the use it is questionable if the sole import without the intention to sell or use the tools is covered by Section 10.

“Export” means an actual shipment, transfer, or transmission of devices or access codes out of a country as well as a transfer of devices or access codes within a country with the knowledge or intent that the devices or access codes will be shipped, transferred, or transmitted outside the country. “Distribution” covers such acts as forwarding devices or passwords to others. Procurement for use covers acts related to the active obtaining of passwords and devices. “Making available” refers to an act that enables other users to obtain access to items. It is also intended to cover the creation or compilation of hyperlinks in order to facilitate access to such service.

This provision in general applies not only to devices that are exclusively designed to facilitate the commission of cybercrime but also covers devices that are generally used for legal purposes, where the offenders’ specific intent is to commit cybercrime. The limitation to devices designed solely to commit crimes is too narrow in its extent and can lead to insurmountable difficulties of proof in criminal proceedings, rendering the provision virtually inapplicable or only applicable in rare instances. A clarification that authorized testing shall not be affected was added in subparagraph 3.

Section 10 requires that the offender is carrying out the offences intentionally. In addition to the regular intent with regard to the acts covered Section 10 requires an addition special intent that the device is used for the purpose of committing any of the offences established in part II.

Subparagraph 2 contains a legal presumption that a suspect that is in possession of more than one item mentioned in subparagraph 1 (i) and (ii) is deemed to possess the item with the required criminal intent unless the contrary is proven.

Section 10 requires that the offender is acting without lawful excuse or justification. In this context the clarification in the subsections needs to be taken into consideration. As a consequence legitimate operation of software tools within self-protection measures are not considered to carried out without lawful excuse.

Section 11: Computer-Related Forgery

Most criminal law systems have criminalized the act of forgery of tangible documents. The dogmatic structure of the national legal approaches varies according to jurisdiction. While one concept is based on the authenticity of the author of the document, another is based on the authenticity of the statement. Section 11 aims to protect the security and reliability of electronic data by creating a parallel offence to the traditional forgery of tangible documents and fill gaps in criminal law, as the traditional legal provisions relating to forgery might not apply to electronically stored data.

The target of a computer-related forgery is computer data as defined by Section 3. In this context it is irrespective of whether they are directly readable and/or intelligible. The provision does not only refers to computer data as the object of one of the acts mentioned, but it is also necessary that the acts are resulting in inauthentic data. Section 11Requires,at least with regard to the mental element of the offence, that the data is the equivalent of a public or private document.

Input of data must correspond with the production of a false tangible document. Alteration refers to the modification of existing data. Suppression of computer data denotes an action that affects the availability of data. This can for example be relevant information from a database is blocked during the automatic creation of an electronic document. Deletion corresponds to the definition of the term in Section 4 covering acts where information is removed.

Section11 requires that the offender carries out the offences intentionally and without lawful excuse or justification.

Section 12: Computer-Related Fraud

Fraud is a popular crime in cyberspace and the application of existing provisions to Internet-related cases can be difficult, where traditional national criminal law provisions are based on the falsity of a person, it is in light of this that the working group decided to include a provision criminalising computer-related fraud.

Section 12 contains a list of the most relevant acts of computer-related fraud. It is necessary that the offender’s manipulations produce a direct economic or possessory loss of another person's property including money, tangibles and intangibles with an economic value.

Input of computer data covers all types of input manipulation, such as feeding incorrect data into the computer as well as computer software manipulations and other interferences with the course of data processing. Alteration refers to the modification of existing data. Suppression of computer data denotes an action that affects the availability of data. Deletion refers to the removal of computer data.

Interference with the functioning of a computer system as mention in b) covers acts such as hardware manipulations, acts suppressing printouts and acts affecting recording or flow of data, or the sequence in which programs are run.

Similar to the operation of the other provisions of the legislative text, Section 11 requires that the offender acted intentionally. This intent refers to the manipulation as well as the incidence of consequential financial loss. In addition, Section 12 requires that the offender acted with a fraudulent or dishonest intent in order to gain economic or other benefits for oneself or another. One example for acts excluded from criminal liability due to lack of special intent is commercial practices arising from market competition that may cause economic detriment to one person and benefit to another, but that are not carried out with fraudulent or dishonest intent.

Moreover, Section 12 requires that the offender is acting without lawful excuse or justification.

Section 13: Child Pornography

Section 13 contains a wide criminalisation of acts related to child pornography. The criminalization of child pornography intends to protect several legal interests. Through the criminalization of the production of child pornography the provision aims to protect children from becoming victims of sexual abuse. With regard to the prohibition of acts related to the exchange of child pornography (offering, distributing) as well as the possession of child pornography, the criminalization of such acts aims to destroy the market for such material, as the ongoing demand for new material can motivate offenders to continue the abuse of children. In addition to this, the prohibition of exchange aims to hinder persons from obtaining access to such material and thereby to prevent a trigger effect that with regard to sexual abuse of children.

“Production” means any process of creating child pornography. It is necessary that the production of child pornography is carried out for the purpose of distribution through a computer system. If the offender produces the material for his own use or intends to distribute it in non-electronic form, the Article 9 Convention on Cybercrime is not applicable.

“Offering” covers acts of soliciting others to obtain child pornography. It is not necessary that such material is offered on a commercial basis but implies that the offender offering the material is capable of providing. “Making available” refers to an act that enables other users to obtain access to child pornography. This act can be committed by placing child pornography on websites or connecting to file sharing systems and enabling others to access such material on unblocked storage capacities or folders.

“Distribution” covers the act of forwarding child pornography to others. “Transmitting” covers all communication by means of transmitted signals. “Procuring for oneself or for another” covers any act of actively obtaining child pornography. Possession is the control a person intentionally exercises towards child pornography. It requires that the offender has control which is not only the case with regard to local storage devices but also remote storage devices that he can access and control. Furthermore possession in general requires a mental element as stated in the definition above. “Obtaining access” covers any act of initiating the process of displaying information made available through information and communication technologies. This is for example the case if the offender enters the domain name of a known child pornography website and initiates the process of receiving the information from the first page which goes along with a necessary automated download process. This enables law enforcement agencies to prosecute offenders in cases where they are able to prove that the offender opened websites with child pornography but they are unable to prove that the offender downloaded material. Such difficulties in collecting evidence arise, for example if the offender is using encryption technology to protect downloaded files on his storage media. This provision is also applicable in cases where a consumption of child pornography can take place without download of material. This may be the case if the website enables streaming videos and, due to the technical configuration of the streaming process, does not buffer the received information but discards them right after transmitted information.

The drafters decided to enable countries not to criminalize the conduct described in Section 13 (1) (d)-(f).

Section 14: Identity-Related Crimes

This provision covers major phases of the typical identity-related crimes. Only the phase of obtaining identity-related information is not covered by this provision, such act is covered by other provisions contained in Part II of the Legislative Text.

The term "transfer" covers data transmission processes from one computer to another computer system. This is relevant if databases with identity-related information that have been illegally obtained are transferred to crime groups which organize the sale of such information. "Possession" is the control a person intentionally exercises towards identity-related information. "Use" covers a wide range of practices such as submitting such information for purchase online.

It is necessary that the offender intentionally carries out the act and in addition has special intent to commit, aid or abet an offence.

Section 15: SPAM

This provision addresses the issue of SPAM by criminalising three (3) of the main acts that most SPAM distributions have in common. In addition to limiting the criminalisation to three major acts, the offender can only be prosecuted if the act affects commerce. Variation a) covers initiating the transmission of multiple electronic mails. This criminalises the transfer of mass mailings without the permission of the recipient. The limitation of criminalization to acts carried out without lawful excuse or justification, plays an important role in distinguishing between legitimate mass mailings (like newsletters) and illegal SPAM. Variation b) criminalises the circumvention of anti-SPAM technology by abusing protected computer systems to relay or transmit electronic messages. It is necessary that the offender acts intentionally with regard to deceiving or misleading the recipient or the providers involved. Variation c) covers the circumvention of anti-SPAM technology by falsifying header information. Depending on the kind of manipulation such act can also be covered by Section 11 of the legislative text.

Section15 requires that the offender carries out the offences intentionally and without lawful excuse or justification. Therefore authorized computer testing shall not be criminalized. Due to differing opinions about the necessity to criminalize the distribution of SPAM the drafters decided create the discretion for countries to opt to not criminalize such conduct in Section 15 (2)(a) provided that other effective remedies are available.

Section 16: Disclosure of Details of and Investigation

Confidentiality of investigations can be from great importance having regard to the aims and strategies employed in conducting such activities. This is particularly relevant if investigations have not yet been concluded and the relevant evidence in question could be modified. In this respect this measure accommodates the needs of law enforcement to ensure that the suspect of the investigation is not made aware of the investigation, as well as the right of individuals to privacy. The latter is included to protect the privacy of the data subject or other persons who may be mentioned or identified in that data.

Section 17: Failure to provide assistance

On many occasions law enforcement agencies are dependent upon the assistance of system administrators and other persons with specific knowledge in order to identify the storage location of relevant evidence or in order to obtain access to information stored. Section 20 establishes a coercive measure to facilitate the search and seizure of computer data. Section 17 establishes the consequences for the failure to comply with such obligation. "Failure" in this regard requires that the offender was objective and personally capable of following the order.

Section 18: Harassment utilizing means of electronic communication

Due to its increasing relevance for Caribbean countries the drafters decided to include a provision criminalising harassment utilizing means of electronic communication. The criminalization requires that the offender initiated any electronic communication. An electronic communication is for example initiated if the offender is sending out an e-mail or a message in a chat. The provision further requires that the offender uses a computer system to support severe, repeated and hostile behaviour. Finally the provision requires that the offender is acting with a specific intent (intended to coerce, intimidate, harass, or cause substantial emotional stress).

PART III

Section 19: Jurisdiction

This section outlines a series of criteria for establishing jurisdiction over the criminal offences enumerated in Sections 4-17. Section 19 a) is based upon the principle of territoriality. Territorial jurisdiction is triggered if both the person attacking a computer system and the victim system are located within the same territory or country. The principle will also apply if the computer system attacked is within its territory, even if the attacker is not.

Section 19 b) contains variants of the principle of territoriality. These require each party to establish criminal jurisdiction over offences committed upon ships flying its flag or aircraft registered under its laws. Both principles are already part of principles of jurisdiction outside Cybercrime as ships and aircraft are frequently considered to be an extension of the territory of state. If the crime is committed on a ship or aircraft that is beyond the territory of the flag Party, there is in general no exercise of jurisdiction. Taking into account the increasing connection offered on board planes and ships the principle has the potential to become more relevant in the future.

Section 19 c) is based upon the principle of nationality. The principle of nationality is most frequently applied by civil law countries. It defines jurisdiction if a national commits an offence abroad, the state is obliged to have the ability to prosecute it if the conduct is also an offence under the law of the state in which it was committed or the conduct has taken place outside the territorial jurisdiction of any State.

PART IV

Sections 20 – 27

The successful investigation of Cybercrime requires that law enforcement agencies have access to the appropriate instruments that are necessary to carry out an investigation. The identification of offenders as well as the protection of the integrity of computer data during an investigation contains several inherently unique challenges for law enforcement authorities. The purpose of Part 4 is to improve the national procedural instruments by defining common minimum standards based on best practices within the region as well as international standards. In this context the definition of standards will help national lawmakers to discover possible gaps in the domestic procedural law. Sections 20-27 only define minimum standards and therefore do not preclude the creation of more extensive criminalization on the national level.

Part 4 introduces new investigation instruments (such as Section 27) and also aims to adapt traditional procedural measures (such as Section 20). All instruments referred to aims at permitting the obtaining and/or collection of data for the purpose of conducting specific criminal investigations or proceedings. The instruments described in Part 4 shall not only be used in traditional computer crime investigation but in any investigation that involves computer data and computer systems.

The drafters discussed at great length the importance of safeguards. There was consensus that the application of procedural instruments provided in Sections 20-27 are to be subject to the conditions and safeguards. The drafters discussed the option of whether to include a comprehensive set of safeguards or whether make use of existing safeguards in the national law. As this legislative text is not directly applicable but only provides guidance for the adjustment and harmonisation of national laws and taking into consideration the differences that may exist in the national laws of each Caribbean country the drafters decided not to define safeguards but leave it to the national implementation process to ensure that all conditions or safeguards, which may be provided constitutionally, legislatively, judicially or otherwise, are applicable with regard to the instruments in Part 4. As new instruments might be established during the implementation process, an extension of existing safeguards may be necessary to balance the requirements of law enforcement with the protection of human rights and liberties.

The differences within the legal systems in the Caribbean were not only taken into consideration with regard to safeguards but also with regard to the definition of conditions for the application of instruments. The provisions provide options for adjustment with regard to the authority in charge of ordering the application of an instrument (for example judge, magistrate, law enforcement, police), the basis of action (for example information on oath or affidavit), the level of certainly (for example suspect or believe) as well as the need to respond (for example may or shall). Finally the drafters decided to enable countries to defer from the implementation certain procedures. Having regard to differing standards relating to the ability to intercept communication, the ability to restrict procedural instruments was specifically provided for in this context.

All instruments listed in Sections 20-27 do only apply to investigations within the territory of the investigating state. With regard to the transnational dimension of Cybercrime the drafters discussed the need to add a separate set of provisions that specifically with international cooperation in transnational Cybercrime investigation. However, the drafters decided that as a result of the specific mandate of the working group, the regulation on international cooperation should not be included

Section 20: Search and Seizure

Even in high-tech crime, investigation search and seizure remains an important investigation process. In general, the prevailing domestic criminal procedural laws include powers of search and seize with regard to tangible objects. But as some jurisdictions do not treat computer data as objects and only allow the seizure of tangible items this section aims at modernising domestic laws on search and seizure of stored computer data by establishing an equivalent power relating to stored data.

The aim of Section 20 (1) is to facilitate the process of collecting digital evidence. The provision clarifies that a warrant is necessary to undertake any search operation. It applies to stored computer data. If such warrant is issued it authorises a law enforcement authorities to not only to activate a computer system, or in other form access it, but also to enter the suspect's premises. The application of the process is not limited to cases where conclusive evidence of the commission of an offence can be collected, but is also applicable to such cases where computer data has been acquired by a person as a result of an offence.

To ensure that the wording of the provision does not hinder the application of sophisticated investigation techniques, the drafters decided not to specify the techniques that may be used to search or access a computer system. The term "search includes" but is not limited to seeking, reading, inspecting or reviewing data.

Section 20 (2) enables investigating authorities to extend their search, or obtain similar access to another computer system or part of it, if certain conditions are fulfilled. The drafters decided that such authorisation is necessary as remote storage systems are currently being used with growing frequency. With regard to the limitation of the procedural instruments to national investigations, the provision is not applicable if the relevant information are stored on a computer system outside the territory (even if it can technically be accessed). The provision does not prescribe how an extension of a search shall be undertaken as the determination of this aspect is left to domestic law.

Section 20(3) authorizes the competent authorities to seize or secure digital evidence. The term seize is defined in Section3. In addition to traditional approaches such as seizure of computer hardware (including computer-data storage media) the provision enables investigation authorities to carry out sophisticated and more minimalistic investigations such as the production of a copy of the relevant data. As such measures could lead to the production of multiple copies, additional measures are required. Consequently the competent authorities may include the ability to remove data at its original source and maintain the integrity of the data to ensure that it is not modified during the investigation process.

Section 21: Assistance

The identification of relevant digital evidence is accompanied by unique challenges. This is especially relevant for the identification of physical storage space given the quantity of data that can be processed and stored as well as the possible security measures that were implemented. Assistance from persons with specific knowledge (such as system administrators) about the functioning of a computer system can therefore be indispensible to an investigation. Such cooperation is not only a benefit to the investigating authorities but also to businesses, as without such assistance investigation authorities may be constrained to remain on the searched premises and prevent access to the computer system for long periods of time while undertaking investigations. Such extended duration of an investigation could create an economic burden on legitimate businesses. The drafters therefore decided to create an obligation of such relevant persons possessing knowledge of the functioning of a computer system or measures applied to protect computer data therein. Such assistance is however limited to that which is reasonably required. Section 21 sets out five (5) areas of assistance. However, the drafters found it important to highlight that the rule against self-incrimination hinders the application of the provision in relation to the suspect of the crime.

Section 22: Production Order

Competent authorities have various powerful processes and procedures in which to collect relevant electronic evidence. One of the most powerful processes is the search and seizure of computer data. This may prove to be of particular significance when conducting a search for evidence stored on servers of a hosting provider such procedures can interfere with the operation of the business, (even if the provider is assisting law enforcement in identifying the physical location). It is in light of this that the drafters decided to include an process in Section 22 (a) that compels a person in its territory to provide specified stored computer data. This provision shall not be interpreted as data retention obligation. The application of the provision is not limited to certain categories of data and is applicable with regard to content and traffic data. With regard to the specific regulation of subscriber information in Section 22(b), this category of data is not included in Section 22(a). In order to prevent an abuse of the process the drafters limited requests to those where information is reasonable required. In addition to this criterion, an order by a competent authority (magistrate/judge) is required.

In those cases where investigators are trying to identify a suspect they may not focus on data being generated during electronic communication but rather on subscriber information that enables them to link criminal conduct to a person. The drafters decided to address this issue in a specific subparagraph (Section 22(b)). Section 22(b) is applicable with regard to any personal information about a subscriber or a

person otherwise using an Internet service. As subscriber information will only be available if a service is offered, the obligation to produce such data is limited to the Internet Service Provider. The provision is not limited to subscriber Information that is stored electronically but also covers non-electronic records as well.

Section 23: Expedited Preservation

Computer data that is necessary to identify an offender or prove that a crime has been committed can easily be deleted of modified before investigators are able to secure the evidence. The modification or deletion does not necessarily happen with the intention to shield the offender (for example, traffic data that is relevant for the identification is often deleted automatically within a rather short period of time after the end of a communication as it is not required anymore). Unlike other international approaches (such as the EU Data Retention Directive) the drafters decided not to prescribe the implementation of data retention obligations but to establish a process that enables law enforcement agencies to order the preservation of such data when necessary.

Based on an order given pursuant to Section 23 any person so ordered (apart from the suspect) is obliged to preserve the data that was processed during the operation of the service. Section 23 does not include an obligation on the person in control of the data to transmit the relevant data to the competent authorities. The transmission obligation is regulated in Sections 22 and 24. After receiving the order the controller of such information is not allowed to permit the manual nor the automatic deletion of data specified in the order for a period of seven (7) days. The drafters agreed that this period is sufficient to obtain an order to request the transmission of the relevant data. If the order for expedited preservation is not in due time followed by either an order for extension of the period, nor by a production order, the controller of the data may delete the stored information.

In order to ensure that investigators have an efficient process to prevent the deletion of relevant evidence and taking into account that Section 23 only prevents the deletion of information and does not give law enforcement access to such information the drafters decided not to require a order by a magistrate or judge, but the section enables any police officer to order the expedited preservation. In the view of the fact that the production order (Section 22) requires an order emanating from the competent authority authorized to do so, ensures the rights of the suspect of the investigation are adequately protected.

The period of preservation can be extended one (1) time. Such extension shall be by order of a magistrate or judge.

Section 24: Partial Disclosure

Albeit the drafters in principle agreed to a strict distinction between the authorisation to order the preservation of data (that can be given by any police officer) and the order to transmit the data (that requires an order from a magistrate or judge) they underscored the necessity of ensuring that investigators are able to obtain immediate access to certain traffic data. Without such partial disclosure, investigators would, in some cases, not be able to trace back the offender and preserve more relevant data when more than one provider was involved. Unlike the production order this instrument is limited to traffic data.

Section 25: Collection of Traffic Data

The drafters recognised that traffic data plays an important role in Cybercrime investigation. Monitoring the traffic data generated during the use of Internet services enables investigators to identify the IP-address of an offender and can then attempt to determine his physical location. Section 25 contains two

(2) different approaches: Based on Section 25(1), any person in control of traffic data can be ordered to either collect or record such data or permit and assist a police officer to collect or record such data. Section 25(2) contains a warrant that authorises a police officer to undertake the collection of traffic data. As the collection of traffic data was as controversially discussed as the interception of content data the drafters decided to highlight that countries may in the exercise of their discretion decide not to implement Section 25.

Section 26: Interception of Content Data

In some cases the collection of traffic data is not sufficient in order to secure the successful conviction of the suspect. This is especially relevant in those cases where investigators already know the communication partner and the services used but have no information about the information exchanged. The drafters decided to include a provision enabling the interception of data communication. To ensure a harmonised approach the provision was drafted in accordance with the model legislative text on interception of communication.

Section 26 contains two (2) different approaches. Based on Section 26(a) an ISP can be ordered to record or collect content data. Sec. 26(b) enables law enforcement authorities to carry out the interception. As the provision was controversially discussed within the working group, the drafters decided that countries may decide not to implement Section 26.

Section 27: Forensic Software

During the discussion within the working group the drafters analysed sophisticated investigation methods. After intensive discussion the drafters decided to include a provision authorising investigators to utilize remote forensic software to collect relevant evidence. The drafters recognised that the process is very intrusive and could potentially interfere with fundamental rights of the suspect the drafters decided to include a number of restrictions. Firstly, the use of such software requires that evidence can not be collected by applying other processes. Secondly, an order by a judge or magistrate is required. Thirdly the application needs to contain four key information (Section 27(1)(a)-(d). In addition the authorised acts are limited by both paragraph 1 and 2. The drafters decided to enable countries to implement further restrictions by limiting the application of the instrument to crimes contained in a list Section 27(7) or not implement this provision (Section 27(8)).

PART V

Section 28: No Monitoring Obligation

Internet providers up to a certain degree have the theoretical technical possibility to monitor activities related to their services. Without a clear regulation there is an uncertainty if there is an obligation to monitor activities and if the providers could be prosecuted based on a violation of the obligation to monitor users activities. Apart from possible conflicts with the data protection regulations and the secrecy of telecommunication, such obligation would especially cause difficulties for hosting providers that store thousands of websites. To avoid these conflicts Sec. 28 excludes a general obligation to monitor the transmitted or stored information. The provision solely limits the liability of providers with regard to criminal liability.

Section 29: Access Provider

Based on Section 29, the liability of access providers (Section 29(1)) and router operators (Section 29(2)) is completely excluded as long as they comply with the three conditions defined in Section 29. As a consequence, the access provider is in general not responsible for criminal offences committed by its users. This full exclusion of liability does not release the provider from the obligation to prevent further offence if ordered by a court or administrative authority.

Section 30: Hosting Provider

The drafter took note that the identification of illegal content is a major challenge for the hosting provider. Especially for popular providers that store thousands of websites manual searches for illegal content would be impossible. As a result, the drafters decided to limit the liability of hosting providers. However, unlike the case of the access provider, the liability of the host provider is not generally excluded but only if certain conditions are fulfilled.

Section 30(1)(a) is limiting the liability if the hosting provider expeditiously removes content after receiving an order from any public authority or court. Expeditiously does in general mean in less than 24 hours.

Section 30(1)(b) defines that as long as the hosting provider has no actual knowledge about illegal activities or illegal content stored on his servers, he is not liable. The drafters found it important to point out that an assumption that illegal content could be stored on the servers is not considered equivalent to actually having knowledge of the issue. If information are brought to the attention of a provider they must be concrete and specific enough to enable him to identify the location of the illegal content. If the provider obtains concrete knowledge about illegal activities or illegal content he can only avoid liability if he informs a public authority about the potentially illegal content. Unlike the European Union E-Commerce directive, that established liability if the hosting provider does not remove illegal content after having information about its existence the drafters decided to leave the decision if content is illegal to competent pubic authorities. Countries may specify the competent authority such content needs to be reported to.

Section 30 is not only applicable for the providers that limit their services to renting technical data storage infrastructure. Popular Internet Services like the auction platforms offer hosting services as well. Countries may decide to implement a hotline service where illegal content can be reported.

As the removal of illegal content might depite the illegal nature of the content interfere with contractual obligation of the provider with regard to its customer. Therefore the drafters decided to implement a clarification in Section 30(3) that in those cases where an order was received pursuant to paragraph 1.

Section 31: Caching Provider

Section 31 limits the liability of caching provider. The term caching is in this context used to describe the storage of popular websites on local storage media in order to reduce the bandwidth and make the access to data more efficient – for example by implementing proxy servers. Within this scope a proxy server may service requests without contacting the specified server by retrieving content saved on local storage media from a previous request. The drafters recognised the economic importance of caching and decided to exclude the liability for automatic temporary storage if the provider complies with the conditions defined by Section 31.

Section 32: Hyperlink Provider

Hyperlinks play in important role in connecting and making available internet content. They enable the provider of the hyperlink to guide the user to specific information available online. The hyperlink provides the command for the web browser to open the deposited internet address. Due to the similarities to hosting of content the drafters decided to regulate the liability of hyperlink provider in accordance with the liability of hosting provider (Section 30).

Section 33: Search Engine Provider

Search engine providers offer search services to identify documents of interest by specifying certain criteria. The search engine will search for relevant documents that match the criteria entered by the user. Search engines play an import role in the successful development of the Internet. Content that is made available on a website but is not listed in the search engine's index can only be accessed if the person wishing to access it knows the complete URL. Due to the similarities to access provider the drafters decided to regulate the liability of search engines in accordance with the liability of access provider (Section 29).

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[22]	J Paul
PRESCOD	Kwesi

[22] 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 Frigate Bay, Saint Kitts and Nevis, 19 – 22 July 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 Finance, Investment, Telecommunications and Energy	BOURNE	Reginald
Barbados	Office of Trade Negotiations	BROWNE	Derek
Barbados	Ministry of Trade, Industry and Commerce	NICHOLLS	Anthony
Belize	Ministry of Finance	LONGSWORTH	Michelle
Belize	Public Utilities Commission	PEYREFITTE	Michael
Dominica	Ministry of Information, Telecommunications and Constituency Empowerment	CADETTE	Sylvester
Dominica	Ministry of Legal Affairs	RICHARDS-XAVIER	Pearl
Grenada	National Telecommunications Regulatory Commission	FERGUSON	Ruggles
Grenada	National Telecommunications Regulatory Commission	ROBERTS	Vincent
Guyana	Public Utilities Commission	PERSAUD	Vidiahar
Guyana	Office of the President	RAMOTAR	Alexei
Guyana	National Frequency Management Unit	SINGH	Valmikki
Jamaica	Digicel Group	GORTON	Andrew
Jamaica	Office of the Prime Minister	MURRAY	Wahkeen
Jamaica	Attorney General's Chambers	SOLTAU-ROBINSON	Stacey-Ann
Jamaica	LIME	SUTHERLAND CAMPBELL	Melesia
Saint Kitts and Nevis	Ministry of National Security	ARCHIBALD	Keisha
Saint Kitts and Nevis	Department of Technology	BOWRIN	Pierre
Saint Kitts and Nevis	ICT4EDC Project	BROWNE	Nima
Saint Kitts and Nevis	Government of St. Kitts and Nevis	CHIVERTON	Eurta
Saint Kitts and Nevis	Department of Technology	HERBERT	Christopher
Saint Kitts and Nevis	Ministry of Youth Empowerment, Sports, Information Technology, Telecommunications and Post	LAZAAR	Lloyd
Saint Kitts and Nevis	Ministry of Finance, Financial Intelligence Unit	MASON	Tracey
Saint Kitts and Nevis	Ministry of Sustainable Development	MUSSENDEN	Amicia

Annex 2

Country	Organization	Last Name	First Name
Saint Kitts and Nevis	Ministry of Youth Empowerment, Sports, Information Technology, Telecommunications and Post	PHILLIP	Glen
Saint Kitts and Nevis	Attorney General's Chambers	POWELL WILLIAMS	Tashna
Saint Kitts and Nevis	Ministry of Finance, Financial Intelligence Unit	SOMERSALL-BERRY	Jacqueline
Saint Kitts and Nevis	Ministry of Youth Empowerment, Sports, Information Technology, Telecommunications and Post	WHARTON	Wesley
Saint Lucia	Ministry of Communication, Works, Transport and Public Utilities	DANIEL	Ivor
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	FELICIEN	Barrymore
Saint Lucia	Cable & Wireless (Saint Lucia) Ltd.	LEEVY	Tara
Saint Lucia	The Attorney General's Chambers	VIDAL-JULES	Gillian
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	ALEXANDER	K. Andre
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	FRASER	Suenel
Suriname	Telecommunicatiebedrijf Suriname (TELESUR)	JEFFREY	Joan
Suriname	Telecommunicatie Autoriteit Suriname	LETER	Meredith
Suriname	Ministry of Justice and Police	SITLADIN	Vyaiendra
Suriname	Ministry of Transport, Communication and Tourism	SMITH	Lygia
Trinidad and Tobago	Office of the Prime Minister, Information Division	MAHARAJ	Rishi
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)	HOPE	Hallam
Caribbean ICT Virtual Community (CIVIC)	ONU	Telojo
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

Annex 2

HIPCAR Consultants Participating in the Workshop

Last Name	First Name
GERCKE	Marco
MORGAN[23]	J Paul
PRESCOD	Kwesi

[23] 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