Final Report

on


DRAFT

Grenada

April 2012

HIPCAR

Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean
This document has been produced with the financial assistance of the European Union. The views expressed herein do not necessarily reflect the views of the European Union.

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.

©ITU 2012

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.
Acknowledgements


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

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

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

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

HIPCAR’s international consultant, Dr. Marco Gercke, prepared the comparative law analysis on cybercrime for Grenada; based on this analysis, the project’s regional consultant, Ms. Suenel Fraser, developed the proposed cybercrime policy and bill for the country – adapted from the HIPCAR Model Policy Guidelines and Model Legislative Text while also taking account of the bills developed under the OECS/EGRIP project as well as considering national needs. These documents were reviewed, discussed and adopted by broad consensus at the national stakeholder consultation meetings on cybercrime, interception of communications and e-evidence held in Grenada on 15-16 February 2012 and on 27-30 March 2012.

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

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

**INTRODUCTION** ........................................................................................................................................... 7

1.1 **THIS REPORT** ....................................................................................................................................... 7

1.2 **THE IMPORTANCE OF FIGHTING CYBERCRIME** ............................................................................. 7

1.3 **THE LEGISLATIVE ENVIRONMENT AND EGRIP** ............................................................................... 9

**SECTION II: NATIONAL POLICY AND EXISTING LEGISLATION** .............................................................. 10

2.1 **OVERVIEW OF EXISTING LEGISLATION** ..................................................................................... 10

2.2 **NATIONAL ICT STRATEGY AND ACTION PLAN 2006-2010** ......................................................... 11

**SECTION III: STAKEHOLDER CONSULTATIONS** ....................................................................................... 12

3.1 **FIRST STAKEHOLDER CONSULTATION / CAPACITY BUILDING WORKSHOP** .......................... 12

3.2 **PRINCIPAL FINDINGS** ..................................................................................................................... 13

**SECTION IV: PROPOSED COMPUTER CRIME AND CYBERCRIME BILL 2012** ........................................ 13

4.1 **GENERAL OVERVIEW** .................................................................................................................... 13

4.2 **PRELIMINARY** .................................................................................................................................... 13

4.3 **OFFENCES** ....................................................................................................................................... 13

4.4 **JURISDICTION** ................................................................................................................................. 14

4.5 **PROCEDURAL LAW** ....................................................................................................................... 14

4.6 **LIABILITY** ....................................................................................................................................... 14

**SECTION V: SECOND STAKEHOLDER CONSULTATION/ VALIDATION WORKSHOP** .............................. 14

5.1 **OVERVIEW** ...................................................................................................................................... 14

**SECTION VI: CONCLUSIONS AND RECOMMENDATIONS** ....................................................................... 15

6.1 **CONCLUSIONS** .............................................................................................................................. 15

6.2 **RECOMMENDATIONS** .................................................................................................................... 15

**ANNEXES** ................................................................................................................................................ 16

Annex 1 **COMPARATIVE LAW ANALYSIS** .............................................................................................. 16

Annex 2 **COMPUTER CRIME AND CYBERCRIME BILL** ............................................................................. 62

Annex 3 **PROPOSED CYBERCRIME POLICY** .......................................................................................... 94

Annex 4 **PARTICIPANTS AT FIRST STAKEHOLDER CONSULTATION WORKSHOP** ........................... 103

Annex 5 **PARTICIPANTS AT CONSULTATION AT MINISTRY OF LEGAL AFFAIRS** .............................. 105

Annex 6 **PARTICIPANTS AT SECOND STAKEHOLDER CONSULTATION/VALIDATION WORKSHOP** .... 106
Section I: Introduction

1.1 This Report

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

The HIPCAR Model Cybercrime 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 providers.

It will function most effectively with the simultaneous enactment of the Interception of Communications legal Framework and the passage of the Electronic Evidence framework which were reviewed, discussed and validated during the Grenada - HIPCAR workshops on 15-16 February and 27-29 March 2012. As these are closely related and dependent on each other to address the concerns of Cybercrime /Electronic Crimes, the Government of Grenada has decided to focus on these work areas to ensure that robust legal frameworks are implemented based on international and regional best practices.

This report deals with Cybercrime and takes account of accepted international and regional best practices. By reflecting national, regional and international best practices and standards while ensuring compatibility with the prevailing legal system in Grenada. It is aimed at meeting and responding to the specific requirements of Grenada, taking account of the regional Model Policy Guidelines and Legislative Texts developed under the HIPCAR project.

1.2 The Importance of 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. 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.

---

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

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

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\(^3\). 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\(^4\). In the last few years, the debate has been dominated by new, very sophisticated methods of committing crimes such as “Phishing\(^5\)”, “Botnet\(^6\) Attacks” and the emerging use of technologies that are more difficult for law enforcement to investigate, such as “Voice-over-IP (VoIP) communication\(^7\)” and “Cloud Computing\(^8\)”.

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\(^9\) 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 ability to act when these services are attacked or abused in other ways. This was underscored by the recent cybercrime event experienced in Grenada in March, where data being sent from one party to another was intercepted by a third party. At the moment Grenada is without the necessary framework to investigate and prosecute this “crime”. Hence this experience shows that 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


\(^5\) 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.

\(^6\) Botnets is a short term for a group of compromised computers running software that are under external control. For more details, see Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4.


Grenada 8
operate with impunity has therefore become a key challenge in preventing cybercrime\textsuperscript{10}. 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\textsuperscript{11}, which infected millions of computers worldwide\textsuperscript{12}. 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\textsuperscript{13}.

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\textsuperscript{14}. In 2005, the number of Internet users in developing countries surpassed the number in the industrialised nations\textsuperscript{15}. 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\textsuperscript{16}. 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.

### 1.3 The Legislative Environment and EGRIP

The Electronic Government for Regional Integration Project (EGRIP) is a project designed to “to promote the efficiency, quality, and transparency of public services in the beneficiary countries, through the delivery of regionally integrated e-government applications that take advantage of economies of scale”\textsuperscript{17}.

The Project which became effective on June 18, 2009 is funded through the World Bank and implemented by the Organisation of Eastern Caribbean States (OECS), in the form of Special Drawing Rights (SDRs) loans to each participating country.

Grenada along with Dominica, Saint Lucia and lately, St. Vincent and the Grenadines are among the OECS participating/beneficiary states.

\textsuperscript{10} 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: \url{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.

\textsuperscript{11} For more information, see \url{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.

\textsuperscript{12} BBC News, “Police close in on Love Bug culprit”, 06.05.2000.


\textsuperscript{14} 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: \url{www2007.org/workshops/paper_106.pdf}.


\textsuperscript{16} 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.

\textsuperscript{17} See \url{http://www.oecs.org/projects/egrip/what-is-the-egrip}
Under the EGRIP Project, a total of six (6) draft bills have been prepared for the beneficiary states as follows:

- Data Protection Bill
- Electronic Crimes Bill
- Electronic Evidence Bill
- Electronic Filing Bill
- Electronic Transaction Bill
- Electronic Funds Transfer Bill

Although Grenada currently has no enacted legislation specifically addressing any of these areas, the Government, based on its stated mission to “…put information and communication technologies (ICT) at the center of Grenada’s social and economic development…” has now commenced the simultaneous review of the EGRIP Draft Bills on Electronic Evidence and Electronic Crimes as well as the Model Policy Guidelines and Legislative Texts, produced under Stage 1 of the HIPCAR Project, in relation to Electronic Evidence, Cybercrime and Interception of Communications.

Section II: National Policy and Existing Legislation

2.1 Overview of Existing Legislation

Grenada currently has no enacted legislation which speaks specifically to computer crimes and/or cybercrime. Nonetheless, there are existing legislations with a few provisions which can possibly be interpreted in the context of cybercrime. One such piece of legislation is the Criminal Code.

The Criminal Code contains certain provisions and definitions, as reflected in the comparative law analysis hereto annexed, which may be given a wide enough interpretation to extend to certain acts of cybercrime. An example of this is Section 24, which defines “Damage” as including “not only damage to the matter of a thing, but also any interruption of the use thereof, or any interference therewith, by which the thing becomes permanently or temporarily useless, or by which expense is rendered necessary in order to render the thing fit for the purposes for which it was used or maintained”. This provision is comparable to Section 7 of the proposed Cybercrime Bill which criminalizes acts which, inter alia, “damages or deteriorates computer data, renders computer data meaningless, useless or ineffective, obstructs, interrupts or interferes with the lawful use of computer data”.

Other provisions may be found in Section 64 and 65 of the Grenada Telecommunications Act, respectively, which makes it an offence for a person to impede, prevent or obstruct any investigation being carried out by the Commission; or to refuse to produce any document, record, thing, or who destroys or alters, or causes to be destroyed or altered, any document, record or thing required to be produced under the Act. This is similar to Section 17 of the proposed Cybercrime Bill.

Although not enacted, mention should be made of the drafted Electronic Transactions Act, dated May 14th 2008. This Act, by Section 43, captioned ‘Misuse of Computer’, makes it an offence for “a person who knowingly and with intent to commit an offence against this Act, or an offence involving property, fraud or dishonesty, causes a computer to perform any function for the purpose of access to any program or data held in that computer in relation to an electronic transaction”. This provision is very limited in that it fails to address the novel ways in which ICT is being used in the commission of known crimes such as copyright infringement, also referred to as piracy, murder and identity theft, inter alia, and new ICT specific crimes such as spoofing and denial of access, etc.

14 ICT Strategy and Action Plan 2006-2010
However, given the many changes which have taken place in the area of Cybercrime globally, new and comprehensive technology neutral legislation is required to ensure that Grenada is in line with international and regional best practices as provided in the HIPCAR Model Cybercrime Legislative Text.

Thus, although there are currently a few legislative provisions which may, to a limited degree, be adapted for the purposes of combating cybercrime, it is also clear that it is necessary for Grenada to implement more comprehensive cybercrime legislation, consistent with technological advancements and which will be effective in bolstering the confidence of would be investors in its information economy and society.

The Government of Grenada has, therefore, used this opportunity to benefit from the expertise of key stakeholders across the Caribbean region and internationally, who developed Model Policy Guidelines and Legislative Text in Cybercrime, in order to review and modernize its national ICT legislative framework with support under Stage 2 of the HIPCAR Project.

This has provided the basis for proposed national policies and legislations which have been developed and adapted respectively, from the HIPCAR Model Policy Guidelines and Legislative Texts to suit the Grenada context, as a result of the HIPCAR stakeholder consultation workshop held on 15-16 February 2012 and consultation/validation workshop on 27-30 March 2012.

### 2.2 National ICT Strategy and Action Plan 2006-2010

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

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

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

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

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

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

- Recognition of electronic records - evidentiary weight
- Writing
- Original form
- Signatures

---

19 Footnote 18 supra at page 7
Section III: Stakeholder Consultations

3.1 First Stakeholder Consultation / Capacity Building Workshop

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

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

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

During the presentations on cybercrime, participants commented on many of the provisions of the EGRIP Draft. Some participants commented on the provisions of section 10 of the Draft which criminalized the writing of malicious codes. It was felt that this provision extended to persons who wrote such codes for the purposes of testing their security systems and as such would have an unintended effect on such persons.

There were also concerns expressed about the criminalizing of prank calls under section 16 of the draft, which it was felt should be dealt with under the Telecommunication Act instead.

With regard to the proposed Bill, based on the HIPCAR Model Legislative Text, it was suggested that the words “other than a suspect” be deleted from section 17, as the provisions against self incrimination in the Grenada Criminal Code made this unnecessary. In the same section the word “permit” was replaced with the word “provide”.

20 Hosted by the Government of Grenada and co-organized with the National Telecommunications Regulatory Commission and the HIPCAR project.
Some ISPs expressed some concerns regarding the costs of intercepting content data in section 26. It was advised that that issue would be dealt with by regulations and not the substantive Act.

3.2 Principal Findings

Based on the discussions and comments from the participants and the general tenor of the stakeholder consultation workshop, the HIPCAR Model Legislative Text and Policy Guidelines on Cybercrime seemed to have gained acceptance as the model text to be transposed into national legislation. Stakeholders expressed some concerns with the drafting style employed by the EGRIP Draft with resulted in difficulties in interpretation of provisions. There were some general concerns with the use of the word “electronic” in many of the provisions, some of which, it was felt, could envelope ordinary everyday household gadgets such as lighting systems and home security systems.


4.1 General Overview

The Computer Crime and Cybercrime Bill, hereinafter referred to as the “Cybercrime Bill” or “the Bill”, is a result of the review of the existing criminal law of Grenada as it relates to computer crime and cybercrime, and is intended to introduce and facilitate the harmonization of cybercrime legislation in Grenada by ensuring its conformity with the HIPCAR Model Policy Guidelines and Legislative Text. It is intended to ensure that existing offences and laws concerning investigative powers and admissibility of evidence in judicial proceedings adequately apply, and if not to recommend the necessary changes to deal with the novel and sophisticated forms of criminal activity. The Bill is divided into five parts which cover the following:

- Preliminary
- Offences
- Jurisdiction
- Procedural law
- Liability

4.2 Preliminary

The Bill, which is consistent with the HIPCAR Model Legislative Text and conforms to international best practice, uses terminology which is technology neutral and broad enough to encompass technological developments in a rapidly changing environment. This part of the Bill is divided into two sections namely the “Short Title” which gives the correct name of the Bill and the “Definitions”, which explains the technical meanings of words as they are used in the context of the Bill.

4.3 Offences

The Bill creates new and specific offences not covered in any of Grenada’s existing legislations. These offences are cybercrime and computer crime specific offences and include, inter alia, identity related crimes, SPAM, and illegal data interference. The Bill also recognises the economic impact such offences can have on a small society such as Grenada and as such imposes penalties ranging from fines of $50,000 to $200,000 and from three (3) years to ten (10) years imprisonment.

Grenada 13
Section V

4.4 Jurisdiction

This Part, which captures any act or omission done or made in Grenada, also enlarges the courts jurisdiction to Grenadians who engage in activities prohibited under the Act, but who at the material time were not within the state of Grenada.

Jurisdiction is also extended to vessels and crafts registered in Grenada, aboard which the act or omission occurred and whether or not by a Grenadian.

4.5 Procedural Law

This part sets out the procedural requirements for investigating cybercrime, and takes into consideration the temporary nature of this type of evidence and how quickly it can be lost. As such it makes provisions for expedited preservation of this type of evidence and the partial disclosure of traffic data, under sections 23 and 24 respectively. In this regard, it empowers a police officer, on reasonable grounds, to expedite same.

The Bill also recognises the potential for abuse of the powers granted hereunder and thus employs certain safeguards which include, time limits on orders granted as in section 27.

4.6 Liability

This part exempts certain types of service providers from criminal liability, given the intermediary roles they play in the transmission of communications. These include caching providers, access providers and hosting providers. It places no obligation on service providers to monitor communications being transmitted over their networks.

Section V: Second Stakeholder Consultation/ Validation Workshop

5.1 Overview

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

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

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

The Consultants also met separately with the legal staff and Permanent Secretary from the Ministry of Legal Affairs, the Police, the Director of Public Prosecutions (DPP), members of the Grenada Cabinet (including the Attorney General) and members of the Opposition.
The feedback from the different groups of stakeholders was very positive. The legal staff of the Ministry of Legal Affairs, the DPP and the Police, were all anxious to know how soon the legislations would be implemented, as they felt that the new legislations would assist them in carrying out their functions more effectively, i.e. the investigation and subsequent prosecution of cases and perpetrators respectively.

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

Section VI: Conclusions and Recommendations

6.1 Conclusions

In light of the findings stated in Section III and for the purposes of regional and international harmonization to facilitate regional and international cooperation in combating cybercrime, the Proposed Computer Crime and Cybercrime Bill is essential legislation required to enable Grenada to create a secure environment for investors while at the same time promoting the confidence of the public in the security of conducting transactions online.

6.2 Recommendations

The following are recommended:

- Adaptation of the model legislative text on cybercrime to suit the Grenada context;
- National sensitization campaign to raise public awareness of cybercrime and to educate stakeholders and the general public on the provisions of the cybercrime act;
- Training for law enforcement to familiarize same with their duties and procedural requirements under the act;
- Training for law enforcement in the investigation of cybercrime and the handling of cyber evidence;
- Training for the Magistracy and Judiciary to familiarize same with technical terms associated with cybercrime.
## Annex 1

### COMPARATIVE ANALYSIS OF CYBERCRIME LEGISLATION IN GRENADE, HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME, COMMONWEALTH MODEL LAW AND EGRIP E-CRIMES

MARCH 2012

**Legend:**
- **Green:** Provision in the local legislation is fully in line with HIPCAR
- **Grey:** Provision in the local legislation requires review
- **White:** Provision in the local legislation is going beyond HIPCAR (and not contained in HIPCAR)
- **Red:** Provision of HIPCAR not contained in the local legislation

<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PART 1 - PRELIMINARY</strong></td>
<td><strong>PART 1 - PRELIMINARY</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DEFINITIONS</strong></td>
<td>Sec. 3 - Definitions</td>
<td>Sec. 3 - Definitions</td>
<td>Sec. 2 - Interpretation</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ACCESS</strong></td>
<td></td>
<td></td>
<td>&quot;access&quot; in the context of an electronic system means to communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of the electronic system;</td>
<td>The definition provided by EGRIP is differing from international standards that define access as entering a computer system. To make use of is in general not considered access of a computer system but use. The reason for the differentiation is that the protected legal instruments are different.</td>
<td></td>
</tr>
<tr>
<td><strong>ACCESS PROVIDER</strong></td>
<td>[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;</td>
<td></td>
<td></td>
<td>HIPCAR introduces a definition of access provider as it differentiates between in regard of the liability.</td>
<td></td>
</tr>
<tr>
<td><strong>CAPTURE</strong></td>
<td></td>
<td></td>
<td>Sec. 11 (2)</td>
<td>The EGRIP provision covers visual</td>
<td></td>
</tr>
<tr>
<td>TITLE</td>
<td>GRENADA</td>
<td>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</td>
<td>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</td>
<td>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>---------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>CHILD</td>
<td>Sec. 2</td>
<td>“child” means a person under the age of eighteen</td>
<td>Sec. 3</td>
<td>(3) Child shall mean any person under the age of eighteen (18) years.</td>
<td>Sec. 10 (3)</td>
</tr>
<tr>
<td>CHILD PORNOGRAPHY</td>
<td>Sec. 10 (3)</td>
<td>“child pornography” includes material that visually depicts: a. a child engaged in sexually explicit conduct; b. a person who appears to be a child engaged in sexually explicit conduct; or c. realistic images representing a minor engaged in sexually explicit conduct.</td>
<td></td>
<td></td>
<td>Grenada legislation does not provide a definition of child pornography. Neither does EGRIP. EGRIP does in particular not define if virtual child pornography and realistic images are covered.</td>
</tr>
<tr>
<td>COMPUTER SYSTEM</td>
<td>(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</td>
<td>“computer system” means a device or a group of inter-connected or related devices, including the Internet, one or more of which, “electronic system” means an electronic device or a group of interconnected or related devices, one or more of which, pursuant to an</td>
<td></td>
<td></td>
<td>The definitions provided by HIPCAR, the COMMONWEALTH Model Law and EGRIP are similar.</td>
</tr>
</tbody>
</table>

HIPCAR introduces a definition of caching provider as it differentiates between in regard of the liability.
<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMPUTER DATA</td>
<td></td>
<td>which, pursuant to a program, performs automatic processing of data or any other function.</td>
<td>pursuant to a program, performs automatic processing of data or any other function;</td>
<td>electronic program, performs automatic processing of data and includes an electronic storage medium;</td>
<td>HIPCAR, EGRIP and Commonwealth provide a similar definition.</td>
</tr>
<tr>
<td>COMPUTER DATA STORAGE MEDIUM</td>
<td></td>
<td>(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.</td>
<td>“computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;</td>
<td>“data” includes representations of facts, information or concepts that are being prepared or have been prepared in a form suitable for use in an electronic system including electronic program, text, images, sound, video and information within a database or electronic system;</td>
<td>The current legislation in Grenada and EGRIP do not provide a definition of data storage media. Such definition might be useful taking into account the relevance of seizing storage data media that can not be considered to be a computer system.</td>
</tr>
<tr>
<td>CONTAMINANT</td>
<td></td>
<td>(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.</td>
<td>“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;</td>
<td>“contaminant” means a set of electronic instructions that are designed—</td>
<td>Neither the current legislation in Grenada, HIPCAR nor the COMMONWEALTH model Law provide a definition of contaminant.</td>
</tr>
<tr>
<td>CRITICAL INFRASTRUCTURE</td>
<td></td>
<td>(8) Critical infrastructure means computer systems, devices, networks, computer programs, computer data, so vital to the country that the</td>
<td>Sec. 14 (3)</td>
<td>For the purposes of this section “sensitive electronic system” is an electronic system used directly in</td>
<td>Both HIPCAR and EGRIP address the issue of critical infrastructure. However, while HIPCAR uses the widely accepted term “critical</td>
</tr>
<tr>
<td>TITLE</td>
<td>GRENADA</td>
<td>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</td>
<td>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</td>
<td>4th DRAFT EGRIP ELECTRONIC CRIMES BILL</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>-----------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>DAMAGE</td>
<td>Sec. 24 – Penal Code</td>
<td>“Damage” includes not only damage to the matter of a thing, but also any interruption of the use thereof, or any interference therewith, by which the thing becomes permanently or temporarily useless, or by which expense is rendered necessary in order to render the thing fit for the purposes for which it was used or maintained.</td>
<td>connection with or necessary for—(a) the security, defence or international relations of [Member State]; (b) the existence or identity of a confidential source of information relating to the enforcement of criminal law; (c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, courts, public transportation or public key infrastructure; (d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services; or (e) the purpose declared as such by the Minister by Order published in the Gazette.</td>
<td>“damage” includes modifying, deleting, erasing, suppressing, changing location or making data temporarily unavailable, halting an electronic system or choking the networks;</td>
<td>Both HIPCAR and the Commonwealth Model Law do not provide a definition of the term “damage”. The Provision provided under the Grenada Penal Code is broader and does not only cover damages related to a computer system.</td>
</tr>
<tr>
<td>DECRYPTION</td>
<td></td>
<td></td>
<td>“decryption” means the process of transforming or unscrambling encrypted data from its unreadable and incomprehensible format to its plain version;</td>
<td></td>
<td>The current legislation in Grenada, HIPCAR and Commonwealth do not provide a provision of decryption as they do not address encryption in criminal law.</td>
</tr>
<tr>
<td>DECRYPTION INFORMATION</td>
<td></td>
<td></td>
<td>“decryption information” means information or technology that</td>
<td></td>
<td>The current legislation in Grenada, HIPCAR and Commonwealth do not</td>
</tr>
<tr>
<td>TITLE</td>
<td>GRENADA</td>
<td>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</td>
<td>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</td>
<td>4th DRAFT EGRIP ELECTRONIC CRIMES BILL</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>-----------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>DEFAMATION</td>
<td>Sec. 254 – Penal Code (1) Matter is defamatory which imputes to a person any crime, or misconduct in any public office, or which is likely to injure him in his occupation, calling or office, or to expose him to general hatred, contempt or ridicule.</td>
<td>“defamation” means defamation within the meaning of [ ]; Grenada provides a definition of “matter of defamatory”. EGRIP does not provide a definition but refer to national law. HIPCAR and COMMONWEALTH do not provide a definition.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DEVICE</td>
<td>(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.</td>
<td></td>
<td></td>
<td></td>
<td>HIPCAR provides a definition of device as the term is used in relation to the criminalization of “illegal devices”.</td>
</tr>
<tr>
<td>ELECTRONIC</td>
<td></td>
<td>“electronic” means relating to technology having electrical, digital, magnetic, optical, biometric, electrochemical, wireless, electromagnetic, or similar capabilities; EGRIP does not refer to the term “computer” and computer “systems” but “electronic” systems. There are two possible implications. As the term is broader “electronic device” would for example a light or household devices that are not capable of processing data. This could lead to an overlapping with other provisions that follow a slightly broader approach. The second possible implication is that as the term “computer system” and “computer crime” is more widely accepted it could be more difficult for other countries to access the</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TITLE</td>
<td>GRENADA</td>
<td>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</td>
<td>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</td>
<td>4th DRAFT EGRIP ELECTRONIC CRIMES BILL</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------</td>
<td>--------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>---------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ELECTRONIC DATABASE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;electronic database&quot; means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by an electronic system or electronic network and are intended for use in an electronic system or electronic network;</td>
</tr>
<tr>
<td>ELECTRONIC DEVICE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;electronic device&quot; is any hardware that accomplishes its functions using any form or combination of electrical energy;</td>
</tr>
<tr>
<td>ENCRYPTED DATA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;encrypted data&quot; means data which has been transformed or scrambled from its plain version to an unreadable and incomprehensible format, regardless of the technique utilized for transformation or scrambling, and irrespective of the medium in which such data occurs or can be found for the purposes of protecting the content of such data;</td>
</tr>
<tr>
<td>ELECTRONIC MAIL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Sec. 5 (2) For the purpose of this section, the term “electronic mail” or “electronic message” means a message or information created or transmitted or received on an electronic system or electronic device including attachments in text,</td>
</tr>
</tbody>
</table>

Legislation in Grenada and identify the relevant provisions if they need to submit requests for international cooperation.

See the comment related to "electronic".

See the comment related to "electronic".

See the comment related to "decryption".

EGRIP provides a provision defining electronic mail/electronic message.
<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENCRYPTION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>“encryption” means the process whereby data is transformed or scrambled from its plain version to an unreadable or incomprehensible format, regardless of the technique utilized for such transformation or scrambling and irrespective of the medium in which such data occurs or can be found for the purposes of protecting such data; “function” includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within an electronic system;</td>
</tr>
<tr>
<td>HIPCAR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>See the comment related to “decryption”.</td>
</tr>
<tr>
<td>HOSTING PROVIDER</td>
<td></td>
<td>[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.</td>
<td></td>
<td></td>
<td>HIPCAR introduces a definition of hosting provider as it differentiates between in regard of the liability.</td>
</tr>
<tr>
<td>HYPERLINK</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HIPCAR introduces a definition of hyperlink as it differentiates between in regard of the liability – including</td>
</tr>
</tbody>
</table>

HIPCAR provides a clarification ("includes but it not limited to") related to the term hinder as the drafter found it necessary to ensure that even acts such as cutting the electricity supply is included.

HIPCAR provides a clarification ("includes but it not limited to") related to the term hinder as the drafter found it necessary to ensure that even acts such as cutting the electricity supply is included.

HIPCAR introduces a definition of hosting provider as it differentiates between in regard of the liability.

HIPCAR introduces a definition of hyperlink as it differentiates between in regard of the liability – including
<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERCEPTION</td>
<td></td>
<td>Image that contains information about another source and points to and causes to display another document when executed.</td>
<td></td>
<td></td>
<td>Hyperlink provider.</td>
</tr>
<tr>
<td>(13) INTERCEPTION</td>
<td></td>
<td>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.</td>
<td></td>
<td></td>
<td>HIPCAR introduces a clarification with regard to the criminalization of illegal interpretation as well as authorization for lawful interception of content data.</td>
</tr>
<tr>
<td>MALICIOUS CODE</td>
<td></td>
<td>“Malicious code” means an electronic program or a hidden function in a program that infects data with or without attaching its copy to a file and is capable of spreading over an electronic system with or without human intervention including virus, worm or Trojan horse;</td>
<td></td>
<td></td>
<td>EGRIP contains a definition of malicious code as it criminalizes the production of acts like the transmission of malicious code. HIPCAR like other regional standards (such as the Council of Europe Convention on Cybercrime and the Commonwealth Model Law) follow a different approach and do not focus on certain tools but on acts (such as damaging) and results (such as interference with the functioning of a computer system). Notice: In addition the definition is in so far possibly causing difficulties as only tools are covered that have the ability to “spread” over an electronic system. Various malicious software does not have this self-replication ability and are therefore not covered by the definition.</td>
</tr>
<tr>
<td>MOBILE PHONE TRACKING</td>
<td></td>
<td>“Mobile phone tracking” means the tracking of the current position of a mobile phone and includes location based services that discloses the actual coordinates of a mobile phone bearer;</td>
<td></td>
<td></td>
<td>Only the EGRIP Model Legislation provides a definition of mobile phone tracking. Mobile phone tracking is a specific and not necessary computer related crime investigation. In addition the provision is only related</td>
</tr>
<tr>
<td>TITLE</td>
<td>GRENADA</td>
<td>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</td>
<td>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</td>
<td>4th DRAFT EGRIP ELECTRONIC CRIMES BILL</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>------------------------------</td>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>----------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MULTIPLE ELECTRONIC MAIL MESSAGE</td>
<td></td>
<td>(14) Multiple electronic mail messages mean a mail message including E-Mail and instant messaging sent to more that thousand recipients.</td>
<td></td>
<td></td>
<td>to mobile phones – no other processor controlled device with location services.</td>
</tr>
<tr>
<td>PLAIN VERSION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HIPCAR criminalizes the distribution of SPAM. Consequently the drafters included a definition of multiple electronic mail.</td>
</tr>
<tr>
<td>PRIVATE AREA</td>
<td></td>
<td></td>
<td>Sec. 11 (2)</td>
<td></td>
<td>Only EGRIP contains a provision of plain version.</td>
</tr>
<tr>
<td>PUBLISHES</td>
<td></td>
<td></td>
<td>Sec. 11(2)</td>
<td></td>
<td>Only EGRIP contains a provision of publishes.</td>
</tr>
<tr>
<td>REMOTE FORENSIC SOFTWARE</td>
<td></td>
<td>(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.</td>
<td></td>
<td></td>
<td>Over the last years more and more</td>
</tr>
<tr>
<td>SEIZE</td>
<td></td>
<td>(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;</td>
<td>Sec. 11 “seize” includes: (a) make and retain a copy of computer data, including by using onsite equipment; and (b) render inaccessible, or remove, computer data in the accessed computer system; and (c) take a printout of output of computer data.</td>
<td></td>
<td>HIPCAR and the Commonwealth Model Law contain definitions of the term search.</td>
</tr>
</tbody>
</table>

EGRIP contains a provision of plain version.
<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERVICE PROVIDER</td>
<td>[17] Internet service provider means a natural or legal person that provides to users services mentioned in sections 28 – 33 hereof.</td>
<td>“service provider” means: (a) a public or private entity that provides to users of its services the ability to communicate by means of a computer system; and (b) any other entity that processes or stores computer data on behalf of that entity or those users.</td>
<td>“service provider” means– (a) a person who provides an information and communication service including the sending, receiving, storing or processing of the electronic communication or the provision of other services in relation to it through an electronic system; (b) a person who owns, possesses, operates, manages or controls a public switched network or provides telecommunication services; or (c) any other person that processes or stores data on behalf of such electronic communication service or users of such service;</td>
<td>HIPCAR uses the term service provider but provides a broader framework with regard to the liability of service provider. COMMONWEALTH and EGRIP provide a general definition.</td>
<td></td>
</tr>
<tr>
<td>SOURCE CODE</td>
<td></td>
<td>“source code” means the listing of programs, electronic commands, design and layout and program analysis of electronic system in any form;</td>
<td></td>
<td>The current legislation in Grenada, HIPCAR and the Commonwealth Model Law do not provide definitions for source code in relation to criminal law.</td>
<td></td>
</tr>
<tr>
<td>SUBSCRIBER</td>
<td></td>
<td></td>
<td>“subscriber” means a person using the services of a service provider;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUBSCRIBER INFORMATION</td>
<td></td>
<td>“subscriber information” means any information contained in any form that is held by a service provider, relating to subscribers of its services other than traffic data and by which can be established– (a) the type of communication service used, the technical provisions taken thereto</td>
<td></td>
<td>Although HIPCAR and COMMONWEALTH refer to subscriber information they do not define the term. Subscriber information is in general referring to the identity of the person using the service. Although EGRIP clearly states that no traffic data should be provided it refers to data related to</td>
<td></td>
</tr>
<tr>
<td>TITLE</td>
<td>GRENADA</td>
<td>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</td>
<td>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</td>
<td>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
<td>-------------------------------------------</td>
<td>------------------------------------------------</td>
<td>---------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>TRAFFIC DATA</td>
<td></td>
<td>(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.</td>
<td>“traffic data” means computer data: (a) that 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 type of underlying services.</td>
<td>and the period of service; (b) the subscriber’s identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; or (c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement;</td>
<td>the type of communication services used – and these are in general traffic data (as clearly stated by the definition of traffic data provided in the EGRIP legislation as well as Commonwealth and HIPCAR Model Law. The provision might therefore lead to an overlapping with provisions referring to traffic data.</td>
</tr>
<tr>
<td>TRANSMIT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>THING</td>
<td>Verification required</td>
<td>(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.</td>
<td>&quot;thing&quot; includes: (a) a computer system or part of a computer system; and (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;</td>
<td>Sec. 11 (2) a) “transmit” means to electronically send a visual image with the intent that it be viewed by a person or persons;</td>
<td>Only EGRIP provides a definition of transmit. The provision is only related to images and does not include audio files.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HIPCAR, EGRIP and the COMMONWEALTH Model Law provide a similar definition.</td>
</tr>
</tbody>
</table>

HIPCAR – Cybercrime
<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4th DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UNDER CIRCUMSTANCES VIOLATING PRIVACY</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ILLEGAL ACCESS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sec. 4</td>
<td></td>
<td>Sec. 5 – Illegal Access</td>
<td>Sec. 4. Access and Interception</td>
<td>International best practices such as the Commonwealth Model Law and the HIPCAR Model Legislative Text criminalize the illegal access to whole or part of a computer system</td>
<td></td>
</tr>
</tbody>
</table>

Only EGRIP uses this term.

Only EGRIP provides a definition of unauthorized access. This is in so far surprising as the term “unauthorized access” is not used in relation to illegally accessing a computer system in EGRIP (Sec. 4). The term is only used in Sec. 18 and in the headline of Sec. 19 (although this provision uses the term unlawful purpose).

Only EGRIP uses this term.

for believing that the computer data sought is stored in the other computer system; and
(c) a computer data storage medium

“unauthorized access” means access of any kind by a person to an electronic system or data held in an electronic system which is unauthorized or done without authority or is in excess of authority, if the person is not himself entitled to control access of the kind in question to the electronic system or data and the person does not have consent to such access from a person so entitled.

Sec. 11 (2)
(e) “under circumstances violating privacy” means circumstances in which a person can have a reasonable expectation that—
(i) he or she could disrobe in privacy, without being concerned that an image of his or her private area was being captured; or
(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

International best practices such as the Commonwealth Model Law and the HIPCAR Model Legislative Text criminalize the illegal access to whole or part of a computer system.

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.
<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>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.</td>
<td>punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.</td>
<td>[...] (f) provide assistance to a person to facilitate access to an electronic system or network in contravention of the provisions of this Act; [...]</td>
<td>system. EGRIP follows a similar approach. The main differences are that the provision does not cover access to part of an electronic system and the provision (Sec. 4) includes various offences while international best practices normally provide different provisions for different protected legal interests. <strong>RECOMMENDATION:</strong> Bringing the current legislation in line with international best practices as summarized in the HIPCAR Model Law should be taken into consideration.</td>
</tr>
<tr>
<td>ILLEGAL REMAINING</td>
<td>Sec. 5</td>
<td>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.</td>
<td></td>
<td></td>
<td>Only HIPCAR criminalizes illegal remaining in a computer. The provision was included as during the negotiation about the ECOWAS Directive on Cybercrime the experts realized that if an offender legally access a computer system but then illegally remains logged in the act of entering the system can not be considered illegal. Other regional approaches such as the Draft African Union Convention followed the same approach. <strong>RECOMMENDATION:</strong> Including a provision dealing with illegal remaining based on the HIPCAR Model Law should be taken into consideration.</td>
</tr>
<tr>
<td>DATA INTERFERENCE</td>
<td>Sec. 7</td>
<td>A person who, intentionally without justification</td>
<td>Sec. 6 – Data Interference</td>
<td>Sec. 4. (1) A person shall not knowingly except when lawfully</td>
<td>HIPCAR and the COMMONWEALTH Model Law include a complex list of</td>
</tr>
<tr>
<td>TITLE</td>
<td>GRENADA</td>
<td>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</td>
<td>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</td>
<td>4th DRAFT EGRIP ELECTRONIC CRIMES BILL</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>------------------------------------------</td>
<td>-----------------------------------------------------------</td>
<td>----------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>lawful excuse or justification or in excess of a lawful excuse or justification, does any of the following acts:</td>
<td></td>
<td>recklessly, without lawful excuse or justification, does any of the following acts:</td>
<td>permitted—</td>
<td>acts that are covered such as damaging, deleting, altering or hindering the access to computer data. All those acts are related to the integrity of computer data. Further more international best practice do not require that the offender accesses a computer within the commission of the crime.</td>
<td></td>
</tr>
<tr>
<td>a) damages or deteriorates computer data; or</td>
<td>(a) destroys or alters data; or</td>
<td>(c) introduce or cause to be introduced a contaminant or malicious code into an electronic system or network;</td>
<td></td>
<td>EGRIP follows a different approach. Sec. 4 does first of all not solely focus on computer data but also protect electronic systems. The provision mentions data, electronic database and programs. As databases and programs are subcategories of data the listing may only serve as clarification but is not required as with regard to the criminalization. EGRIP explicitly mentions the introduction of malicious code. International best practices follow a different approach and do not concentrate on the method used to interfere with data but the act and result. As the introduction of a computer virus leads to modification of computer data (as a result of the installation process) it does not require such explicit provision to cover the conduct.</td>
<td></td>
</tr>
<tr>
<td>b) deletes computer data; or</td>
<td>(b) renders data meaningless, useless or ineffective;</td>
<td>(d) damage or cause to be damaged an electronic system or network, data, electronic database or other program residing in such electronic system or network;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c) alters computer data; or</td>
<td>(c) obstructs, interrupts or interferes with the lawful use of data;</td>
<td>(i) willfully destroy, delete or alter information residing in an electronic system or diminish its value or utility or damages by any means; or</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>renders computer data meaningless, useless or ineffective;</td>
<td>or</td>
<td>(j) steal, conceal, destroy or alter or cause a person to steal, conceal, destroy or alter any source code used for an electronic system with an intention to cause damage.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d) obstructs, interrupts or interferes with the lawful use of computer data; or</td>
<td>(d) obstructs, interrupts or interferes with any person in the lawful use of data;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>e) obstructs, interrupts or interferes with any person in the lawful use of computer data; or</td>
<td>or</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>f) denies access to computer data to any person authorized to access it;</td>
<td>(e) denies access to data to any person entitled to it;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.</td>
<td>commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(2) Subsection (1) applies whether the person’s act is of temporary or permanent effect.</td>
<td>(2) Subsection (1) applies whether the person’s act is of temporary or permanent effect.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**RECOMMENDATION:** Bringing the current legislation in line with international best practices as summarized in the HIPCAR Model Law should be taken into consideration. In this regard it is recommended to differentiate between the different protected legal interests and avoid overlapping...
<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>OFFENSIVE MESSAGES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128. - Criminal Code</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Whoever threatens any other person with unlawful harm, with intent to put that person in fear of unlawful harm, shall be liable to imprisonment for one month.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>252. (1) Whoever is convicted of negligent libel shall be liable to imprisonment for six months. (2) Whoever is convicted of intentional libel shall be liable to imprisonment for two years.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>253. A person is guilty of libel who, by print, writing, painting, effigy or by any means otherwise than solely by gestures, spoken words, or other sounds, unlawfully publishes any defamatory matter concerning another person, either negligently or with intent to defame that other person.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>254. (1) Matter is defamatory which imputes to a person any crime, or misconduct in any public office, or which is likely to injure him in his occupation, calling or office, or to expose him to general hatred, contempt or ridicule. (2) In this section, “crime” means any offence punishable on</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sec. 18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. (1) A person shall not send by means of an electronic system or electronic device— a) information that is grossly offensive or has menacing character; b) information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such electronic system or electronic device; or c) electronic mail or an electronic message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages. (2) For the purpose of this section, the term “electronic mail” or “electronic message” means a message or information created or transmitted or received on an electronic system or electronic device including attachments in text, images, audio, video and any other electronic record which may be transmitted with the message. (3) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine (not exceeding one hundred</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The current Criminal Code in Grenada contains several provisions that criminalize offences like defamation, libel and threatening another person. However, some of the provisions focus on acts that may not be applicable with regard to computer and Internet-related conduct. A review should be taken into consideration.

HIPCAR and EGRIP contain provisions that contain acts related to the commission of such crimes to computer technology.

**RECOMMENDATION:** A review of the acts referring to activities such as printing, writing, painting or “any other means otherwise than ..” are applicable to online conduct should be taken into consideration. Such analysis should include the interpretation of the provisions by courts. If required clarifications should be added to all relevant provisions. To ensure consistency this should not be limited to libel and defamation but include all provisions that are referring to similar conduct.
<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IDENTITY RELATED CRIME**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sec. 14</td>
<td>A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification by using a computer</td>
</tr>
<tr>
<td>6. (1)</td>
<td>A person shall not fraudulently or dishonestly make use of an electronic signature, password or other unique identification feature of another</td>
</tr>
</tbody>
</table>

thousand dollars or to imprisonment for a term not exceeding six months or to both].

Both HIPCAR and EGRIP contain provisions addressing identity related crime. EGRIP focuses on criminalizing the unlawful use of signatures.
<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFAMATION</td>
<td>253 - Criminal Code</td>
<td>A person is guilty of libel who, by print, writing, painting, effigy or by any means otherwise than solely by gestures, spoken words, or other sounds, unlawfully publishes any defamatory matter concerning another person, either 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.</td>
<td>person. (2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine of [fifty thousand dollars and imprisonment for a term of six months].</td>
<td>passwords or other unique identification features of another person. Although EGRIP is introducing this provision in context of electronic crimes (&quot;Electronic Crimes Bill&quot;) the provision is also applicable to acts committed without the use of computer systems. The main difference between EGRIP and international best practices is the fact that the offences solely focuses on the use of identity. The UN core expert group on identity-related crime underlined in its reports that there are three main phases: Obtaining, possessing/transferring and finally using identity-related information. HIPCAR follows this best practice and criminalizes various acts ranging from possession to use of such information. RECOMMENDATION: Taking into account the relevance of identities in electronic communication a criminalization of such conduct in line with best practices should be taken into consideration.</td>
<td></td>
</tr>
</tbody>
</table>

The current Criminal Code in Grenada contains provisions that criminalize defamation, libel and threatening another person. However, some of the provisions focus on acts that may not be applicable with regard to computer and Internet-related conduct. A review should be taken into...
<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4th DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>negligently or with intent to defame that other person.</td>
<td></td>
<td>thousand dollars or to imprisonment for a term not exceeding three years or to both].</td>
<td>consideration. EGRIP contains provision that criminalizes the defamation using an electronic system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>254. (1) Matter is defamatory which imputes to a person any crime, or misconduct in any public office, or which is likely to injure him in his occupation, calling or office, or to expose him to general hatred, contempt or ridicule. (2) In this section, “crime” means any offence punishable on indictment under this Code, and any act punishable on indictment under any law in force within the jurisdiction of the Court, and any act, whereassoever committed, which if committed by a person within the jurisdiction of the Court, would be punishable on indictment under any law.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COMPUTER-RELATED FORGERY</td>
<td>107 - Criminal Code (1) Whoever forges or wilfully and without due authority alters a telegram, or utters a telegram knowing the same to be forged or wilfully and without due authority altered, or who transmits by telegraph as a telegram, or utters as a telegram, any message or communication which he or she knows to be not a telegram, shall, whether he or she had or had not an intent to defraud, be liable to a fine of ninety-six dollars.</td>
<td>Sec. 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</td>
<td>Sec. 8. (1) A person shall not, interfere with data or an electronic system with the intention that he, she, or another person uses the data or the electronic system to induce a person to accept the data or an electronic system as genuine and by reason of so accepting it to do or not to do any act to his or her own or any other person’s prejudice or injury. (2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine (not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years</td>
<td>The current Criminal Code of Grenada contains several provisions that criminalize forgery. However, it is uncertain if the criminalized acts mentioned in the provisions are applicable with regard to Internet-related crime. EGRIP includes a provision. The provision criminalizes the interference with data or electronic systems. This is a rather unusual approach as forgery is typically related to documents and methods of payment but not to systems. It is uncertain how for example a computer can be forged.</td>
<td></td>
</tr>
<tr>
<td>TITLE</td>
<td>GRENADA</td>
<td>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</td>
<td>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</td>
<td>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>----------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>300.</td>
<td>Whoever— (a) with intent to defraud, or with intent to defeat, obstruct, or pervert the course of justice, forges any document of any of the following kinds, namely, any will, any document of title to land, any judicial record, any power of attorney, any bank note, bill of exchange, promissory note, or other negotiable instrument, any policy of insurance, or any cheque or other authority for the payment of money by a person carrying on business as a banker; (b) with intent to defraud any person to the amount of ninety-six dollars or upwards, forges any document whatever; or (c) is convicted of being a common forger, shall be liable to imprisonment for fifteen years. 303. Whoever with intent to defraud any person to the amount or value of twentyfour dollars or upwards forges any document whatsoever shall be liable to imprisonment for five years. 304. Whoever forges any document whatsoever, with intent to defraud or injure any person, or with intent to defeat, obstruct, or pervert the course of justice or the due execution</td>
<td>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.</td>
<td>or to both).</td>
<td>HIPCAR follows an approach that can also be found in other wide accepted standards such as the Council of Europe Convention on Cybercrime and the Draft African Union Convention. RECOMMENDATION: A review if the acts referred to in the forgery-related provisions of the Grenada Criminal Code should be taken into consideration. Such analysis should include the interpretation of the provisions by courts. In order to ensure that Grenada is able to cooperate with other countries in international investigations it is recommended to ensure that provisions introduced are in line with international best practices.</td>
<td></td>
</tr>
<tr>
<td>TITLE</td>
<td>GRENADA</td>
<td>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</td>
<td>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</td>
<td>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>--------------------------------------------</td>
<td>------------------------------------------------------------</td>
<td>----------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ELECTRONIC FRAUD</td>
<td>of the law, or with intent to evade the requirements of the law or with intent to commit, or to facilitate the commission of any crime, shall be liable to imprisonment for two years.</td>
<td>Sec. 11</td>
<td>Sec. 9. (1) A person shall not for gain, interfere with data or an electronic system— (a) to induce another person to enter into a relationship; or (b) with intent to deceive a person, which act is likely to cause damage or harm to that person or any other person. (2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years or to both.</td>
<td>Sec. 441 of the Grenada Criminal Code criminalizes fraud by electronic communication. The main difference to international best practices such as the Draft African Convention, the Council of Europe Convention on HIPCAR is the fact that Sec. 441 does only cover acts related to the transmission of communication. The manipulation of computer systems or stored computer data leading to a loss of property is not covered. Compared to international best practices that include three elements (interference with computer systems or data, loss of property and the intent of procuring an economic benefit) EGRIP is following a different dogmatic approach. Sec. 9 is even applicable if – without causing loss and without intent to procure and economic benefit a person interferes with data to induce another person to enter into a relationship. HIPCAR follows international best practices in criminalizing computer-related fraud. <strong>RECOMMENDATION:</strong> The introduction of a provision dealing with computer-related fraud, that goes beyond Art. 441 and is not limited to communication should be taken into consideration.</td>
<td></td>
</tr>
</tbody>
</table>
## MALICIOUS CODE

<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Sec. 10</td>
<td></td>
<td>Sec. 10. (1) A person shall not write, offer, make available, distribute or transmit a malicious code through an electronic system. (2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years or to both.</td>
<td>EGRIP provides a provision that specifically criminalizes the distribution/transmission of a malicious code. As pointed out above, the definition of malicious code in the EGRIP Model Law possibly causing difficulties as only tools are covered that have the ability to “spread” over an electronic system. Various malicious software do not have this self-replication ability and are therefore not covered by the definition. In addition there is significant overlapping between different provisions in the EGRIP Model Law. Sec. 4 for example criminalizes the introduction of a malicious code to a computer network. The transmission of a malicious code through a computer network is therefore covered by Art. 10 and Art. 4. International best practices follow a different approach and do not criminalize specific methods but focus on acts and results. They do for example criminalize the modification of computer data that is caused by the installation of malicious software. HIPCAR, like other international standards also criminalizes the production, sell and distribution of tools that can be used to commit a crime.</td>
</tr>
<tr>
<td>TITLE</td>
<td>GRENADA</td>
<td>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</td>
<td>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</td>
<td>4th DRAFT EGRIP ELECTRONIC CRIMES BILL</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------</td>
<td>-------------------------------------------</td>
<td>---------------------------------------------------</td>
<td>--------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>VIOLATION OF PRIVACY</td>
<td>Verification required</td>
<td>Part II of this law, such as for the authorized testing or protection of a computer system.</td>
<td></td>
<td></td>
<td>Sec. 11. (1) A person who, intentionally or knowingly captures, publishes or transmits the image of a private area of a person without his or her consent, under circumstances violating the privacy of that person, commits an offence and is liable on summary conviction to a fine of fifty thousand dollars and to imprisonment for a term of three years.</td>
</tr>
<tr>
<td>MISUSE OF ENCRYPTION</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Sec. 12 12. (1) A person shall not for the purpose of commission of an offence or concealment of incriminating evidence, knowingly and wilfully encrypt any incriminating communication or data contained in an electronic system relating to the offence or incriminating evidence. (2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine (not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years or to both).</td>
</tr>
<tr>
<td>TERRORIST</td>
<td>Verification required</td>
<td>-</td>
<td>-</td>
<td>15. A person who— a) with intent to threaten the unity, integrity, security or sovereignty of [Member State] or to strike terror in the people or any section of the people by—</td>
<td>Only EGRIP criminalizes attacks carried out with a specific terrorist related intent.</td>
</tr>
</tbody>
</table>
(i) denying or causing the denial of access to any person authorised to access an electronic system;
(ii) attempting to penetrate or accessing an electronic system without authorisation or exceeding authorised access; or
(iii) introducing or causing to introduce any contaminant, and by means of such conduct causes or is likely to cause death or injury to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the [critical information infrastructure] relating to the security of [Member State], or
b) knowingly or intentionally penetrates or accesses a electronic system without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or electronic database that is restricted for reasons for the security of [Member State] or foreign relations, or any restricted information, data or electronic database, with reasons to believe that such information, data or electronic database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of [Member State], the security of [Member State], friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of
**PRANK CALLS**

16. (1) A person shall not make calls to any law enforcement authority or emergency services with the purpose of giving false and misleading information.

(2) A person making a call to any law enforcement or emergency services shall not–

(a) use a caller identification service to transmit misleading or inaccurate caller identification information service;

(b) mask their voice; or

(c) provide a fake phone number to the call recipient.

(3) A person who contravenes subsection (1) or (2) commits an offence and is liable on summary conviction to a fine of [five thousand dollars or to imprisonment for six months or to both].

**CHILD PORNOGRAPHY**

<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4th DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
</table>
| Sec. 133 - Criminal Code | Sec. 13 | Sec. 10 – Child Pornography | | | | 13. (1) A person shall not–

(a) publish or transmit or cause to be published or transmitted material in an electronic form which depicts a child engaged in sexually explicit act or conduct or an image that is indistinguishable from, that of a child engaged in a sexually explicit act; or

(b) create text or digital images, collect, seek, browse, download, | The current Grenada Criminal Code does not explicitly criminalize acts related to child pornography but only mentions indecent material. A review should therefore be taken into consideration (see comment below). HIPCAR criminalizes several acts related to child pornography. With regard to the acts covered Sec. 10 HIPCAR is following international best practices as such as Optional |

(e) sells, or distributes, or offers for sale or distribution any profane, indecent, or obscene book, paper, print, or representation; | Sec. 13 | | | | | Only EGRIP introduces such provision. What is surprising is that the provision is limited to calls while EGRIP intends to introduce legislation related to electronic crime. If it was the intention not only to introduce crimes related to computer systems but the entire telecommunication industry further regulations would be required. |
<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4th DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATA ESPIONAGE</td>
<td>Sec. 8</td>
<td>pornography through a computer system; d) procures and/or obtain child pornography through a computer system for oneself or for another person; Possesses child pornography in a computer system or on a computer-data storage medium; or 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 defence to a charge of an offence under paragraph (1) (a) or (1)(c) 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).</td>
<td>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 defence to a charge of an offence under paragraph (1) (a) or (1)(c) if the person establishes that the child pornography was a bona fide law enforcement purpose.</td>
<td>advertise, promote, exchange or distribute material in an electronic form depicting a child in obscene or indecent or sexually explicit manner or an image that is indistinguishable from, that of a child engaged in a sexually explicit act; c) cultivate, entice or induce a child to an online relationship with another child or an adult for a sexually explicit act or in a manner that may offend a reasonable adult on the electronic system; d) facilitate abusing a child online, or e) record in an electronic form own abuse or that of others pertaining to sexually explicit act with a child.</td>
<td>Protocol to the UN Convention on the Protection of Children, the Council of Europe Convention on Cybercrime, the Commonwealth Model Law and the Draft African Convention. Sec. 10 HIPCAR is applicable with regard to images as well as audio recordings. EGRIP is following a different approach. Most of the acts mentioned (such as “seek” and “browse” are rather unusual. In addition the provision does only refer to text and images and does not include audio files. RECOMMENDATION: A review of the existing legislation should be taken into consideration to verify if child pornography is covered by the existing law and if the provision is applicable with regard to computer related acts. In order to increase the ability to cooperate internationally the introduction of a specific provision (that is in line with international best practices) should be taken into consideration. Such provision should use widely accepted language.</td>
</tr>
<tr>
<td>40</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TITLE</td>
<td>GRENADA</td>
<td>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</td>
<td>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</td>
<td>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>--------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>---------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>SYSTEM INTERFERENCE</td>
<td>62. — (1) No person shall remove, injure, or destroy any telecommunications network, or telecommunications apparatus, except to apparatus in accordance with this Act.</td>
<td>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.</td>
<td>Sec. 7 – System Interference (1) A person who intentionally or recklessly, without 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. In subsection (1) “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, deleting or altering computer data;</td>
<td>4. (1) A person shall not knowingly except when lawfully permitted– c) damage or cause to be damaged an electronic system or network, data, electronic database or other program residing in such electronic system or network; d) disrupt or cause disruption of an electronic system or network; e) deny or cause the denial of access to a person authorised to access an electronic system or network by any means; f) provide assistance to a person to facilitate access to an electronic system or network in contravention of the provisions of this Act; g) charge the services availed of by a person to the account of another person by tampering with or manipulating an electronic system or network; h) willfully destroy, delete or alter information residing in an electronic system or diminish its value or utility or damages by any means; or</td>
<td>RECOMMENDATION: An introduction of a provision criminalizing illegal acquisition of computer data should be taken into consideration.</td>
</tr>
<tr>
<td>TITLE</td>
<td>GRENADA</td>
<td>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</td>
<td>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</td>
<td>4th DRAFT EGRIP ELECTRONIC CRIMES BILL</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>DISCLOSURE OF DETAILS OF AN INVESTIGATION</td>
<td>Verification required</td>
<td>Sec. 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 d) 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.</td>
<td>Sec. 21 – Confidentiality (1) An Internet service provider who without lawful authority discloses: (a) the fact that an order under section 13, 15, 16, 17, 18 and 19 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.</td>
<td>29. (1) A service provider shall not be liable for any actions taken or any information provided or disclosed to the Police or other law enforcement agencies in accordance with this Part. (2) A service provider who without lawful authority discloses: (a) the fact that an order under this part has been made; or (b) anything done under the order; or (c) any data collected or recorded under the order; commits an offence and is liable on conviction to a fine of fifty thousand dollars.</td>
<td>The COMMONWEALTH Model Law, HIPCAR and EGRIP follow a similar approach with regard to the criminalization of details of an investigation.</td>
</tr>
</tbody>
</table>

**RECOMMENDATION:** Taking into account the threat that the disclosure of an on-going investigation could hinder investigations the introduction of a provision criminalizing the illegal disclosure of details of an investigation should be taken into consideration.
<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON Cybercrime</th>
<th>COMMONWEALTH MODEL LAW on COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4th DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ELECTRONIC STALKING</strong></td>
<td>128.</td>
<td>Sec. 18</td>
<td>Sec. 17</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Whoever threatens any other</td>
<td>person</td>
<td>(1) A person, who 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.</td>
<td>A person who, with intent to harass, intimidate, torment, or embarrass any other person, makes an electronic communication to such other person or a third party:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>other person with unlawful</td>
<td>with</td>
<td>(2) A country may decide not to criminalize harassment utilizing means of electronic communication.</td>
<td>a) Using any lewd, lascivious, indecent, or obscene words, images, or language, or suggesting the commission of any lewd or lascivious act anonymously or repeatedly whether or not conversation occurs; or</td>
<td></td>
<td></td>
</tr>
<tr>
<td>harm, with intent to put that</td>
<td>intent</td>
<td></td>
<td>b) Threatening to inflict injury on the person or property of the person communicated with or any member of his or her family or household;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| person in fear of unlawful    | to       |                                            | is guilty of an offence and liable on conviction to [a fine of $50,000 or to imprisonment for a term of five years or to both.]
| harm, shall be liable to      | imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. |
| imprisonment for one month.  |          |                                            | (2) An offence committed under this section may be deemed to have been committed either at the place from which the communication was made or at the place where the communication was received. |
| **ILLEGAL DEVICES / ACCESS** | 10.     | Sec. 10                                     | Sec. 19                                                       |                                        |          |
| CODES                        |         | (1) A person commits an offence if the person: | A person shall not disclose or obtain a password, an access code or any other means of gaining access to an electronic system or data with intent to obtain wrongful gain or inflict wrongful loss to a person or for any unlawful purpose. |
|                              |         | 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: | (2) A person who contravenes subsection (1) commits an offence |
|                              |         | (i) a device, including a computer program, that is designed | |
|                              |         | (ii) a computer system or data with intent to obtain wrongful gain or inflict wrongful loss to a person or for any unlawful purpose. |

The current Grenada Criminal Code criminalizes threatening others. The provision is drafted in a technology neutral way. It should be verified if it is applicable with regard to acts committed online.

EGRIP and HIPCAR contain a provision criminalizing harassment. The main difference between EGRIP and HIPCAR is that Sec. 17(1)(a) is focussing on words, images or language while HIPCAR does not specify by which means the act is committed.

**RECOMMENDATION:** A review of the existing legislation should be taken into consideration to verify if it is applicable with regard to online conduct. If it is not applicable an amendment of the provision should be taken into consideration.

HIPCAR and the COMMONWEALTH Model Law follow international best practices when it comes to the criminalization of illegal devices. They both criminalize the production and distribution of tools designed for the purpose of committing crime as well as access codes.

EGRIP follows a different approach and solely focuses on access codes...
<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1. 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</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. A computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. A person found guilty of an offence against this section is liable to a penalty of imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. 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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. A country may decide not to criminalize illegal devices or limit the criminalization to devices listed in a Schedule.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. and passwords</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**RECOMMENDATION:** The introduction of a provision criminalizing illegal devices should be taken into consideration. However, such approach should only be undertaken if this can be integrated into an existing structure related to the criminalization of preparatory acts.
<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sec. 60 – Telecom Act</td>
<td>Any message transmitted over a public telecommunications network, shall be confidential and shall not be intercepted or interrupted without the consent of the sender, or without a court order made under this Act or any other enactment.</td>
<td>Sec. 6 [1] A person who, intentionally without 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.</td>
<td>Sec. 8 – Illegal Interception A person who, intentionally without 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 that are carrying computer data; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.</td>
<td></td>
<td>Sec. 60 of the Telecommunications Act criminalizes the illegal interception. But the provision is limited to the interception of messages transmitted over a public network. The provision is not applicable with regard to other forms of data communication. HIPCAR and the COMMONWEALTH Model Law follow a similar approach and criminalize both the illegal interception of non-public transmissions as well as electromagnetic emissions. Although illegal interception is a typical cybercrime and highly relevant due to the increasing use of wireless Internet access points EGRIP does not contain a provision criminalizing illegal interception. RECOMMENDATION: An amendment of the existing provision should be taken into consideration to not only cover the interception of messages but any data communication.</td>
</tr>
<tr>
<td>SPAM</td>
<td></td>
<td>Sec. 15 [1] A person who, intentionally, without 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</td>
<td>Sec. 5 [1] A person shall not send by means of an electronic system or electronic device— […] (c) electronic mail or an electronic message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages.</td>
<td></td>
<td>HIPCAR is following a broad approach. Sec. 15 criminalizes various acts related to SPAM that reflect best practices from national legislation in other regions – such as the US. This includes abusing trusted computer systems as relay. EGRIP is following a similar approach but it is limited to sending electronic</td>
</tr>
<tr>
<td>TITLE</td>
<td>GRENADA</td>
<td>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</td>
<td>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</td>
<td>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>---------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>----------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>any electronic mail or Internet service provider, as to the origin of such messages, or</td>
<td>For the purpose of this section, the term “electronic mail” or “electronic message” means a message or information created or transmitted or received on an electronic system or electronic device including attachments in text, images, audio, video and any other electronic record which may be transmitted with the message.</td>
<td>mail for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages. This covers a significant part of SPAM mails but is not addressing the issue in broad way (such as HIPCAR does).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
<td>(3) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine (not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding six months or to both).</td>
<td>RECOMMENDATION: A broader criminalization of SPAM, differentiating between the different acts, should be taken into consideration.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(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.</td>
<td>(b) fail to comply with a request made by a police officer under this section.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sec. 64 – Telecoms Act</td>
<td>Sec. 23</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>A person who, in any manner, impedes, prevents, or obstructs any investigation being carried out by the Commission under this Act commits an offence and is liable, on conviction on indictment to a fine of eight thousand dollars or to imprisonment for a period not exceeding six months.</td>
<td>[...] A person shall not—</td>
<td>Sec. 64 Telecommunications Act criminalises obstructions to any investigation. The major difference to Sec. 17 is the fact that Sec. 64 is limited to investigations carried out by the Commission. HIPCAR provides a criminalization of the failure to permit assistance. EGRIP follows a similar approach but restricted to search and seizure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>65. A person who----- (a) refuses to produce any document, record, thing, or any information required by the Commission under this Act; or (b) destroys or alters, or cause to be destroyed or altered,</td>
<td>(a) obstruct a police officer in the exercise of the police officer’s powers under this section; or</td>
<td>RECOMMENDATION: It should be verified if the failure to provide assistance is also criminalized by other Acts in Grenada. If not an amendment of the legislation should be taken into consideration.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(b) fail to comply with a request made by a police officer under this section.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sec. 17</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(2) A country may decide not to criminalize the failure to permit assistance provided that other effective remedies are available.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
any document, record or thing required to be produced under this Act; commits an offence and is liable, on conviction on indictment, to a fine not exceeding five thousand dollars or to imprisonment for a period not exceeding six months.

67. A person who—— (a) refuses or fails, without reasonable excuse, to appear before the Commission, having been required to do so; or

<table>
<thead>
<tr>
<th>JURISDICTION</th>
<th>Verification required</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sec. 19 – Jurisdiction</td>
</tr>
<tr>
<td></td>
<td>This Act applies to an act done or an omission made:</td>
</tr>
<tr>
<td></td>
<td>a) in the territory of [enacting country]; or</td>
</tr>
<tr>
<td></td>
<td>b) on a ship or aircraft registered in [enacting country]; or</td>
</tr>
<tr>
<td></td>
<td>c) by a national of [enacting country] outside the jurisdiction of any country; or</td>
</tr>
<tr>
<td></td>
<td>d) 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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>JURISDICTION</th>
<th>Verification required</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sec. 4 - Jurisdiction</td>
</tr>
<tr>
<td></td>
<td>This Act applies to an act done or an omission made:</td>
</tr>
<tr>
<td></td>
<td>a) in the territory of [enacting country]; or</td>
</tr>
<tr>
<td></td>
<td>b) on a ship or aircraft registered in [enacting country]; or</td>
</tr>
<tr>
<td></td>
<td>c) by a national of [enacting country] outside the jurisdiction of any country; or</td>
</tr>
<tr>
<td></td>
<td>d) 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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>JURISDICTION</th>
<th>Verification required</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sec. 3. This Act applies where— (a) an offence under this Act is committed in [Member State]; (b) any act of preparation towards an offence under this Act or any part of the offence is committed in [Member State] or where any result of the offence has an effect in [Member State]; (c) an offence under this Act was committed by a [ ] national or a person resident or carrying out business in [Member State] or visiting [Member State] or staying in transit in [Member State]; (d) an offence under this Act is committed in relation to or connected with an electronic system</td>
</tr>
</tbody>
</table>

HIPCAR and the COMMONWEALTH Model Law define jurisdiction in line with international best practices. EGRIP is using a drafting style that not only differs from EGRIP and the Commonwealth Model Law but also from other international best practices. One example is Sec. 3 (a). The described principle is called “principle of nationality”. However, unlike most codifications EGRIP does not mention the term “territory”. Sec. 3 (c) is first of all implementing the principle of nationality (“committed by a [ ] nation). But the further elements are overlapping with the (more accurate) principle of territoriality in Sec. 3 (a). The provision does not establish jurisdiction on ships or aircrafts.

> Grenada 47
<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>or data in [Member State] or capable</td>
<td>registered in the enacting country.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>of being connected, sent to, used by</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>or with an electronic system in [Member State]; or</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(e) an offence under this Act is committed</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>by any person, of any nationality or citizenship or in any place outside or inside [Member State], having an effect on the security of [Member State] or its nationals, or having universal application under international law, custom and usage.</td>
<td></td>
</tr>
<tr>
<td>PART IV PROCEDURAL LAW</td>
<td></td>
<td></td>
<td></td>
<td>(2) For the purposes of subsection (1), data includes traffic data and subscriber information.</td>
<td></td>
</tr>
<tr>
<td>EXPEDITED PRESERVATION</td>
<td></td>
<td>Sec. 23 – Preservation of data</td>
<td>Sec. 17 – Preservation of data</td>
<td>HIPCAR and the Commonwealth Model Law follow a similar approach and enable the expedited preservation of traffic data. Such measure – that needs to be carried out in an expedited manner – can be ordered by a police or law enforcement officer. This is international best practice.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If a [law enforcement] [police] 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] 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.</td>
<td>(1) A police officer may apply to a [Magistrate] [Judge in Chambers] for an order for the expeditious preservation of data that has been stored or processed by means of an electronic system, where there are reasonable grounds to believe that the data is vulnerable to loss or modification and where such data is required for the purposes of a criminal investigation or the prosecution of an offence.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sec. 17 – Preservation of data</td>
<td>20. (1) A police officer may apply to a [Magistrate] [Judge in Chambers] for an order for the expedited preservation of traffic data. Such measure – that needs to be carried out in an expedited manner – can be ordered by a police or law enforcement officer. This is international best practice. EGRIP follows a different approach. The measure can only be applied if a magistrate or judge issues an order.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(1) If a police officer is satisfied that:</td>
<td>(2) For the purposes of subsection (1), data includes traffic data and subscriber information.</td>
<td>RECOMMENDATION: Expedited preservation should be included as an investigation instrument.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(a) data stored in a computer system is reasonably required for the purposes of a criminal investigation; and</td>
<td>(3) An order made under subsection (1) remains in force–</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(b) there is a risk that the data may be destroyed or rendered inaccessible;</td>
<td>a) until such time as may be reasonably be required for the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>the police officer may, by written notice given to a person in control of the computer system, require the person to ensure that the data specified in the notice be preserved for a period of up to 7 days as specified in the notice.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TITLE</td>
<td>GRENADA</td>
<td>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</td>
<td>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</td>
<td>4th DRAFT EGRIP ELECTRONIC CRIMES BILL</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>----------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>PARTIAL DISCLOSURE OF TRAFFIC DATA</td>
<td>Sec. 24</td>
<td>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.</td>
<td>Sec. 16 – Disclosure of Stored Traffic Data If a police officer is satisfied that data stored in a computer system is reasonably required for the purposes of a criminal investigation, the 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 communication to identify: (a) the service providers; and (b) the path through which the communication was transmitted.</td>
<td>21. A police officer (not below the rank of superintendent) may, for the purposes of a criminal investigation or the prosecution of an offence, apply to a [Magistrate] [Judge in Chambers] for an order for the disclosure of– (a) any preserved data, irrespective of whether one or more service providers were involved in the transmission of the data; (b) sufficient data to identify the service providers and the path through which the data was transmitted; or HIPCAR and the COMMONWEALTH Model Law provide a provision dealing with the partial disclosure of certain traffic data. This approach is in line with international best practices. EGRIP follows a different approach. Sec. 21 EGRIP is first of all not limited to traffic data but any data. Further more the procedural instrument can not be applied by police or law enforcement officers but require an order of a judge. This requirement can seriously interfere with the effectiveness of instrument and is not in line with international best practice. RECOMMENDATION: Partial disclosure should be included as an investigation instrument.</td>
<td></td>
</tr>
<tr>
<td>PRODUCTION ORDER</td>
<td>Sec. 22</td>
<td>If a [magistrate/judge] is satisfied on the basis of an application by a [law enforcement] [police] that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the [magistrate/judge] may order that:</td>
<td>Sec. 15 – Production Order If a magistrate is satisfied on the basis of an application by a 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</td>
<td>22. (1) If the disclosure of data is required for the purpose of a criminal investigation or the prosecution of an offence, a police officer (not below the rank of superintendent) may apply to a [Magistrate] [Judge in Chambers] for an order compelling– (a) a person to submit specified data HIPCAR, the COMMONWEALTH Model Law and EGRIP follow a similar approach when it comes to production order. RECOMMENDATION: Production order should be included as an investigation instrument.</td>
<td></td>
</tr>
</tbody>
</table>

Grenada 49
### SEARCH AND SEIZURE

<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
</table>
|       |     | 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. | 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; and  
   b) an Internet service provider in [enacting country] produce information about persons who subscribe to or otherwise use the service; and  
   c) a person in the territory of [enacting country] who has access to a specified computer system process and compile specified computer data from the system and give it to a specified person. | in that person’s possession or control, which is stored in an electronic system;  
   b) a service provider offering its services to submit subscriber information in relation to the services in that service provider’s possession and control. |
|       |     | Sec. 55 – Telecom Act  
   (1) Where a magistrate is satisfied by information on oath that—  
   (a) there is reasonable ground for suspecting that an offence under this Act has been committed or is about to be committed; and  
   (b) evidence of the commission of that offence is to be found on any premises, vehicles, vessel or | Sec. 20  
   (1) If a [judge or 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 [judge or magistrate] [may] [shall] issue a warrant authorizing a [law | Sec. 12 – Search and Seizure  
   (1) If a 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 | Sec. 23.  
   (1) Where a police officer [not below the rank of superintendent] has reason to believe that stored data would be relevant for the purposes of an investigation or the prosecution of an offence, the police officer may apply to a [Magistrate] [Judge in Chambers] for the issue of a warrant to enter any premises to access, search and seize that data. |
<p>|       |     | | | | Sec. 55 of the Grenada Telecommunications Act contains a provision dealing with search and seizure. However, the provision does not include specific procedures related to the search and seizure of electronic data. HIPCAR and the Commonwealth Model Law provide specific investigation instruments related to the search and seize of electronic evidence. This includes international |</p>
<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>aircraft specified in the information, he may issue a search warrant authorising the inspector named in the warrant, with or without a police officer, to enter and search the premises, vehicles, vessel or aircraft specified in the information and examine, test or seize any apparatus and equipment.</td>
<td>person as a result of an offence; the magistrate [may] [shall] issue a warrant authorising a [law enforcement] 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.</td>
<td>(2) In the execution of a warrant under subsection (1), the powers of the police officer shall include the power to— (a) access, inspect and check the operation of an electronic system; (b) use or cause to be used an electronic system to search any data contained in or available to the electronic system; (c) access any information, code or technology which has the capability of transforming or unscrambling encrypted data contained or available to an electronic system into readable and comprehensible format or text for the purpose of investigating any offence under this Act or any other offence which is disclosed in the course of the lawful exercise of the powers under this section; (d) require a person in possession of the decryption information to grant the police officer access to such decryption information necessary to decrypt data required for the purpose of investigating the offence; (e) seize or secure an electronic system.</td>
<td>best practice related to the seizure of electronic evidence which includes copying data and rendering it inaccessible (see the definition of seizure provided by HIPCAR and the COMMONWEALTH Model Law).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(2) Any document, telecommunications apparatus or other thing seized pursuant to a search warrant shall— (a) where legal proceedings are not commenced within a period of thirty days from the date of seizure of the document, telecommunications apparatus or thing be returned to the owner; or (b) where legal proceedings are commenced before the expiry of the thirty days, be kept until the conclusion of those proceedings.</td>
<td>(3) The police officer or another authorized person may refuse to</td>
<td></td>
<td>EGRIP is following a different approach. It also provides specific investigation instruments for the search of information (that includes activating a computer system). But the provision does not include international best practices with regard to the seizure of such evidence. Further more it does not allow the extension of search.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Where a licensee is convicted of an offence under this Act in respect of any document, telecommunications apparatus or thing seized under this Part the Court may order the forfeiture of that document, telecommunications apparatus of thing.</td>
<td>The implementation of specific search and seizure procedures should be taken into consideration.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TITLE</td>
<td>GRENADA</td>
<td>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</td>
<td>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</td>
<td>4th DRAFT EGRIP ELECTRONIC CRIMES BILL</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>----------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>PROVIDING ASSISTANCE</td>
<td>Sec. 21</td>
<td>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 is the subject of a search under section 21 must permit, and assist if reasonably required and requested by the person authorized to make the search by:</td>
<td>give access or provide copies if he or she has reasonable grounds for believing that giving the access, or providing the copies: (a) would constitute a criminal offence; or (b) would prejudice: (i) the investigation in connection with which the search was carried out; or (ii) another ongoing investigation; or (iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations.</td>
<td>(4) A person shall not– (a) obstruct a police officer in the exercise of the police officer’s powers under this section; or (b) fail to comply with a request made by a police officer under this section.</td>
<td>HIPCAR and the COMMONWEALTH Model Law contain a provision that requires people in possession or control of a computer system to provide assistance to investigators. HIPCAR clarifies that this provisions applies to anybody except the suspect of a crime.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a) providing information that enables the undertaking of measures referred to in section 20;</td>
<td></td>
<td></td>
<td>EGRIP also contains requirements to provide assistance. But this is limited to the disclosure of keys to encrypted material. Such requirement – if applied with regard to the suspect - may interfere with fundamental human rights – such as the ban on self-incrimination.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>b) accessing and using a computer system or computer data storage medium to search any computer data available to or in the system;</td>
<td></td>
<td></td>
<td>RECOMMENDATION: With regard to the importance of support from people that have knowledge about</td>
</tr>
<tr>
<td></td>
<td></td>
<td>c) obtaining and copying such computer data;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>d) using equipment to make copies; and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(2) A person who fails without lawful excuse or justification to</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(2) A person who fails without lawful excuse or justification to</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>obtain an intelligible output from a computer system in a plain text format that can be read by a person.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(2) A person who fails without lawful excuse or justification to</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>decrypt data required for the purpose of investigating the offence;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

21. A police officer [not below the rank of superintendent] may, for the purposes of a criminal investigation or the prosecution of an offence, apply to a [Magistrate] [Judge in Chambers] for an order for the disclosure of– […] (c) the electronic key enabling access to or the interpretation of data. | | | | | |

23. […] (2) In the execution of a warrant under subsection (1), the powers of the police officer shall include the power to […] (d) require a person in possession of the decryption information to grant the police officer access to such decryption information necessary to decrypt data required for the purpose of investigating the offence; | | | | |
<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>COLLECTION OF TRAFFIC DATA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>obtaining an intelligible output from a computer system in such a format that is admissible for the purpose of legal proceedings.</td>
<td>permit or assist a person commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.</td>
<td>the functioning of a computer system in investigations the introduction of a provision requiring assistance should be taken into consideration. This could be safeguarded by a criminal law provision providing sanctions if assistance is not provided.</td>
<td></td>
</tr>
</tbody>
</table>
| | Sec. 25  
1) If a [magistrate/judge] is satisfied on the basis of [information on oath/affidavit] that there are reasonable grounds [to suspect/to believe] that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the [magistrate/judge] [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 [magistrate/judge] is satisfied on the basis of [information on oath/affidavit] that there are reasonable grounds to suspect that traffic data is reasonably required for the purposes of a criminal investigation, the [magistrate/judge] [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. | Sec. 19 – Interception of traffic data  
1) If a police officer is satisfied that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the police officer may, by written notice given to a person in control of such data, request that person to:  
a) collect or record traffic data associated with a specified communication during a specified period; and  
b) permit and assist a specified police officer to collect or record that data.  
2) If a magistrate is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds [to suspect] that traffic data is reasonably required for the purposes of a criminal investigation, the magistrate [may] [shall] authorize a police officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means. | 24. Where a police officer [not below the rank of superintendent] has reasonable grounds to believe that any data would be relevant for the purposes of investigation and prosecution of an offence, the police officer may apply to a [Magistrate] [Judge in Chambers] for an order–  
(a) allowing the collection or recording of traffic data, in real time, associated with specified communications transmitted by means of an electronic system; or  
(b) compelling a service provider, within its technical capabilities to effect such collection and recording referred to in paragraph (a) or assist the police officer to effect such collection and recording. |
| | | | | | HIPCAR, the COMMONWEALTH Model Law and EGRIP all provide a procedural instrument that allows the real time collection of traffic data.  
RECOMMENDATION: An implementation of a provision allowing the collection of traffic data should be taken into consideration. |
<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERCEPTION OF CONTENT DATA</td>
<td></td>
<td>Sec. 26</td>
<td>Sec. 18</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
|                           |         | (1) If a [magistrate][judge] is satisfied on the basis of [information on oath][affidavit] that there are reasonable grounds [to suspect][to believe] that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the [magistrate][judge] [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. | (1) If a [magistrate][judge] is satisfied on the basis of [information on oath][affidavit] that there are reasonable grounds [to suspect][to believe] that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the [magistrate][judge] [may][shall]: 
(a) order an Internet service provider whose service is available in [enacting country] through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or  
(b) authorize a police officer to collect or record that data through application of technical means. |
|                           |         | HIPCAR and the COMMONWEALTH Model Law both provide investigation instruments that allow the interception of content data. Such instrument reflects international best practices and is for example also contained in the Draft African Union Convention and the Council of Europe Convention on Cybercrime.  
EGRIP does not contain such instrument.  
RECOMMENDATION: Interception of content data should – possibly restricted to serious offences – be introduced as an investigation instrument. |                                      |          |          |
| FORENSIC SOFTWARE         |         | Sec. 27                                                                                                    | Sec. 44                                                                                   |                                      |          |
|                           |         | (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 5 hereinbelow 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 |
|                           |         |                                                                                                             |                                                                                             |                                      |          |
|                           |         | HIPCAR introduces a provision authorizing investigators – based on a court order – to use advanced investigation instruments such as key-loggers. Similar investigations techniques are used by various countries – including the US.  
RECOMMENDATION: An introduction of a provision allowing the use of remote forensic software – such as keylogger – should be taken |                                      |          |          |
<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4th DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>[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.</td>
<td></td>
<td></td>
<td>into consideration. The application of the provision can be restricted.</td>
</tr>
</tbody>
</table>

(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
<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4th DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>title</td>
<td></td>
<td>section 28 [1] is limited to [3 month]. If</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>the conditions of the authorization is</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>no longer met, the action taken are to</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>stop immediately.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(4) The authorization to install the</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>software includes remotely accessing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>the suspects computer system.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(5) If the installation process requires</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>physical access to a place the</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>requirements of section 21 need to be</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>fulfilled.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(6) If necessary a police officer may</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>pursuant to the order of court granted</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>in (1) above request that the court</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>order an internet service provider to</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>support the installation process.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(7) [List of offences]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(8) A country may decide not to</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>implement section 28.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NO MONITORING OBLIGATION**

|       |         | Sec. 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].                       |                                                              |                                        |          |

**34. EGRIP E-TRANSACTIONS BILL**

(2) An intermediary or electronic commerce service provider shall not be required to monitor any electronic record processed by means of his system in order to ascertain whether its processing would (apart from this section) constitute or give rise to an offence or give rise to civil liability.

**RECOMMENDATION:** Introducing a provision dealing with monitoring obligations should be taken into consideration.

HIPCAR and EGRIP's E-Transactions Bill follow a similar approach with regard to the clarification that Internet Service Provider is not obliged to monitor transactions. However, EGRIP is referring to electronic records.

HIPCAR and EGRIP's E-Transactions Bill follow a similar approach with regard to the clarification that Internet Service Provider is not obliged to monitor transactions. However, EGRIP is referring to electronic records.

HIPCAR and EGRIP's E-Transactions Bill follow a similar approach with regard to the clarification that Internet Service Provider is not obliged to monitor transactions. However, EGRIP is referring to electronic records.

HIPCAR and EGRIP's E-Transactions Bill follow a similar approach with regard to the clarification that Internet Service Provider is not obliged to monitor transactions. However, EGRIP is referring to electronic records.
<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>GENERAL LIABILITY</td>
<td>Sec. 29</td>
<td>(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.</td>
<td>Sec. 34 EGRIP E-TRANSACTIOINS BILL (1) An intermediary or electronic commerce service provider may not be subject to any civil or criminal liability in respect of any information contained in an electronic record in respect of which the intermediary provides services, if the intermediary was not the originator of the record and— (a) he has no actual knowledge that the information gives rise to civil or criminal liability; (b) is not aware of any facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known; or (c) follows the procedure set out in section 35 if the intermediary or electronic commerce service provider— (i) acquires knowledge that the information gives rise to criminal liability, or (ii) becomes aware of facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known.</td>
<td>With regard to the liability of Internet Service Provider EGRIP follows a different concept compared to HIPCAR. HIPCAR differentiates between different type of providers and defines individual liabilities. The EGRIP does not provide such differentiation.</td>
<td></td>
</tr>
<tr>
<td>HOSTING PROVIDER</td>
<td>Sec. 29</td>
<td>(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</td>
<td></td>
<td></td>
<td>With regard to the liability of Internet Service Provider Grenada and EGRIP follow a different concept compared to HIPCAR. HIPCAR differentiates between different type of providers and defines individual liabilities. The Grenada eTransactions Act and the EGRIP do not provide such differentiation.</td>
</tr>
</tbody>
</table>
(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.

RECOMMENDATION: A review of the existing liability regime should be taken into consideration to verify if a differentiated liability should be introduced.

Sec. 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

With regard to the liability of Internet Service Provider Grenada and EGRIP follow a different concept compared to HIPCAR. HIPCAR differentiates between different type of providers and defines individual liabilities. The Grenada eTransactions Act and the EGRIP do not provide such differentiation.

RECOMMENDATION: A review of the existing liability regime should be taken into consideration to verify if a differentiated liability should be introduced.
<table>
<thead>
<tr>
<th>TITLE</th>
<th>GRENADA</th>
<th>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</th>
<th>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</th>
<th>4TH DRAFT EGRIP ELECTRONIC CRIMES BILL</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sec. 31</td>
<td></td>
<td>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:</td>
<td></td>
<td></td>
<td>With regard to the liability of Internet Service Provider Grenada and EGRIP follow a different concept compared to HIPCAR. HIPCAR differentiates between different type of providers and defines individual liabilities. The Grenada eTransactions Act and the EGRIP do not provide such differentiation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(a) the caching provider does not modify the information;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(b) the caching provider complies with conditions of access to the information;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(c) the caching provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(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</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TITLE</td>
<td>GRENADA</td>
<td>HIPCAR MODEL LEGISLATIVE TEXT ON CYBERCRIME</td>
<td>COMMONWEALTH MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME</td>
<td>4th DRAFT EGRIP ELECTRONIC CRIMES BILL</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>---------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>-------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sec. 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.</td>
<td></td>
<td></td>
<td>With regard to the liability of Internet Service Provider Grenada and EGRIP follow a different concept compared to HIPCAR. HIPCAR differentiates between different type of providers and defines individual liabilities. The Grenada eTransactions Act and the EGRIP do not provide such differentiation. <strong>RECOMMENDATION:</strong> A review of the existing liability regime should be taken into consideration to verify if a differentiated liability should be introduced.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sec. 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: 1. does not initiate the transmission; and 2. does not select the receiver of the transmission; and 3. does not select or modify the information contained in the transmission.</td>
<td></td>
<td></td>
<td>With regard to the liability of Internet Service Provider Grenada and EGRIP follow a different concept compared to HIPCAR. HIPCAR differentiates between different type of providers and defines individual liabilities. The Grenada eTransactions Act and the EGRIP do not provide such differentiation. <strong>RECOMMENDATION:</strong> A review of the existing liability regime should be taken into consideration to verify if a differentiated liability should be introduced.</td>
</tr>
</tbody>
</table>
Annex 2

GRENADA

COMPUTER CRIME AND CYBER CRIME BILL

Arrangement of Sections

PART I

PRELIMINARY

1. Short Title
2. Definitions

PART II

OFFENCES

3. Illegal Access
4. Illegal Remaining
5. Illegal Interception
6. Illegal Data Interference
7. Data Espionage
8. Illegal System Interference
9. Illegal Devices
10. Computer-related Forgery
11. Computer-related Fraud
12. Child Pornography
13. Identity-related Crimes
14. SPAM
15. Disclosure of Details of an Investigation
16. Failure to Provide Assistance
17. Harassment Utilizing Means of Electronic Communication
PART III

JURISDICTION

18. Jurisdiction

PART IV

PROCEDURAL LAW

19. Search and Seizure
20. Assistance
21. Production Order
22. Expedited Preservation
23. Partial Disclosure of Traffic Data
24. Collection of Traffic Data
25. Interception of Content Data
26. Forensic Software

PART V

LIABILITY

27. No Monitoring Obligation
28. Access Provider
29. Hosting Provider
30. Caching Provider
31. Hyperlinks Provider
32. Search Engine Provider
GRENADA

BILL NO. OF 2012

AN ACT to provide for the prevention and investigation of computer and network related crime in Grenada.

PART I
PRELIMINARY

1. (1) This Act may be cited as the Computer Crime and Cybercrime Act.

(2) This Act shall come into force on such date as the Governor-General may appoint by Proclamation published in the Gazette.

2. (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 the automatic, intermediate and temporary storing of information, performed for the sole purpose of making more efficient the information’s onward transmission to other users of the service upon their request.

(3) “Child” means any person under the age of eighteen (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.

(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 pads, scanners, digital cameras;

d. output devices such as printers, 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 the characteristic or property of an element, such as a symbol, word, phrase, sentence, or an 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” means mail messages including E-Mails and instant messaging sent to more than a thousand recipients.

(15) “Person” in Section 16 (1) does not include a suspect or an accused person.
(16) “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.

(17) “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. impounding or similarly securing a computer system or part of it or a computer-data storage medium.

(18) “Internet service provider” means a natural or legal person who provides to users services mentioned in sections 27 – 32 hereof.

(19) “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.

(20) “Thing” includes but is 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.

(21) 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

3. (1) A person who intentionally, without lawful excuse or justification or in excess of 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 three years or a fine not exceeding fifty thousand dollars, or both.

4. (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 five years, or a fine not exceeding one hundred thousand dollars, or both.

5. (1) A person who, intentionally without lawful excuse or justification or, in excess of 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 five years, or a fine not exceeding one hundred thousand dollars, or both.

6. A person who, intentionally without lawful excuse or justification or, in excess of 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;
Data Espionage

7. (1) A person who, intentionally without lawful excuse or justification or, in excess of 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 eight years, or a fine not exceeding one hundred and fifty thousand dollars, or both.

Illegal System Interference

8. (1) A person who intentionally, without lawful excuse or justification or, in excess of 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 five years, or a fine not exceeding one hundred thousand dollars or both.

(2) A person who intentionally, without lawful excuse or justification or in excess of 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 twelve years, or a fine not exceeding two hundred and fifty thousand dollars or both.

Illegal Devices

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

a. intentionally, without lawful excuse or justification or, in excess of 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.
commit an offence punishable, on conviction, by imprisonment for a period not exceeding five years, or a fine not exceeding one hundred thousand dollars 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.

10. (1) A person who intentionally, without lawful excuse or justification or, in excess of 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 of whether or not the data is directly readable and intelligible, commits an offence punishable on conviction, by imprisonment for a period not exceeding six years, or a fine not exceeding one hundred and twenty thousand dollars 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 eight years, or a fine not exceeding one hundred and fifty thousand dollars or both.

11. A person who intentionally, without lawful excuse or justification or in excess of 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 ten years, or a fine not exceeding two hundred thousand, or both.

12. (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 obtains 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; and
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 three years, or a fine not exceeding fifty thousand, 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.

13. 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 five years, or a fine not exceeding one hundred thousand dollars, or both.

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

   a. intentionally 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 three years, or a fine not exceeding fifty thousand dollars or both.

15. 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 five years, or a fine not exceeding one hundred thousand dollars or both.
16. (1) A person who intentionally fails without lawful excuse or justification or, in excess of lawful excuse or justification to permit or assist a person based on an order as specified by sections 19 to 21 commits an offence punishable, on conviction, by imprisonment for a period not exceeding two years, or a fine not exceeding two hundred thousand dollars, or both.

17. A person, who 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 behaviour, commits an offence punishable, on conviction, by imprisonment for a period not exceeding three years, or a fine not exceeding fifty thousand dollars or both.

PART III
JURISDICTION

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

   a. in the territory of Grenada; or
   b. on a ship or aircraft registered in Grenada; or
   c. by a national of Grenada outside the jurisdiction of any country; or
   d. by a national of Grenada outside the territory of Grenada, 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

19. (1) If a judge is satisfied on the basis of affidavit that there are reasonable grounds to suspect 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 judge shall issue a warrant authorizing a 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 Grenada.

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

(3) A police officer who is undertaking a search is empowered to seize or similarly secure computer data accessed according to paragraphs 1 or 2.

20. Assistance

(1) 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 19;

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.

21. Production Order

If a judge is satisfied on the basis of an application by a 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 may order that:

a. a person in the territory of Grenada 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 Grenada to produce information about persons who subscribe to or otherwise use the service.

22. Expedited Preservation

If a 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 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 authorizes an extension for a further specified period of time.

23. If a police officer is satisfied that data stored in a computer system is reasonably required for the purposes of a criminal investigation, the 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.

24. (1) If a judge is satisfied on the basis of an application by a police officer, that there are reasonable grounds to suspect that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the judge 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 police officer to collect or record that data.

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

25. (1) If a judge is satisfied on the basis of an application by a police officer, that there are reasonable grounds to suspect that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the judge shall:

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

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

26. (1) If a judge is satisfied on the basis of an application by a police officer, that in an investigation concerning an
offence listed in paragraph 7 below there are reasonable grounds to believe that essential evidence cannot be collected by applying other instruments listed in Part IV but is reasonably required for the purposes of a criminal investigation, the judge shall on application authorize a 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 against 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 are no longer met, the action taken is to stop immediately.

(4) The authorization to install the software includes remotely accessing the suspect’s 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 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) The offences referred to in subsection (1) include:

i. Murder or Manslaughter or treason.

ii. Kidnapping or abduction.
iii. Money laundering contrary to the Proceeds of Crime Act.

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

v. Importing or exporting a dangerous drug in contravention of the Dangerous Drugs Act.

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

vii. Manufacture of, or dealing, in firearms or ammunition in contravention of the Firearms Act.

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


x. Arson.

xi. International Convention on hijacking, terrorist offences etc.

xii. Prevention of Terrorism Act.

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

PART V
LIABILITY

No Monitoring Obligation

27. 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 Grenada.

Access Provider

28. (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.

29. (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.

30. A caching provider is not criminally liable for the automatic, intermediate and temporary storage of information, stored 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 the industry;

   d. the caching provider does not interfere with the lawful use of technology, widely recognised and used by the 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.

31. An Internet service provider who enables the access to information provided by a 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.

32. A provider who makes or operates a search engine that either automatically or, based on entries by others, creates an index of Internet-related content or, makes available electronic tools to search for information provided by a 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.
Explanatory Notes to Cybercrime / e-Crimes Act

INTRODUCTION

1. This Act provides a legal framework for the criminalisation of computer and network related offences. The principal aims of this Act 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 providers.

2. These explanatory explain the contents of the Act, and need to be read in conjunction with it. They explain the importance of the provisions and, where applicable, reflect the discussions within the HIPCAR Working Group. They are not, and are not meant to be, a detailed description of this Act. So, where a Section or part of a Section does not seem to require any comprehensive clarification, comment or reference, or when there was no discussion concerning a particular provision, no detailed explanation is given.

3. The 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.

COMMENTARY ON SECTIONS

PART I

Section 1. Definitions

(1) Access Provider

The responsibility of certain Internet Service Providers are limited in this Act, if their ability to prevent users from committing crimes is limited. It was therefore necessary to differentiate between the different types of providers.

---

21 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).

22 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/ITUD/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. Wherever the words “working group” or “drafters” appear in this document, it refers to the aforementioned Workshop.
Sec. 3 (1) provides 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, intermittently 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 model legislative text, on which this Act is drafted. 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 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 videos, language that enables the coverage of audio, visual or text material is used.

(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. As such, the definition in the Act has been extended to include the internet.

(6) Computer Data

The definition of “computer data” is based on international standards; examples are provided in brackets to ensure that all types of content are covered.

(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. This Act therefore uses an open definition which 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 a broad definition of critical infrastructure has been used in this Act.

(9) Devices

An open ended approach to the application of provisions referring to a device has been used 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. In this Act, 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

In this Act, the criminal responsibility of a “hyperlink” provider is regulated, hence 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. This Act, however, includes some examples for both legitimate acts as well as the types of communication that can be interception.

(14) Multiple Electronic Mail Messages

Given the potential negative impact of SPAM for developing countries, one essential component of the criminalisation of SPAM is the definition of multiple messages. In this regard the Act requires that messages be sent to a minimum of one thousand (1,000) recipients.

(15) Remote Forensic Software

An aspect which was intensively discussed during the negotiations of the model legislative text, was the conduct of sophisticated investigation procedures. As such the definition of “remote forensic software” highlights the possible
fields where such software could be used (keystroke logging and transmission of IP-addresses) but does 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, this definition is elaborated on by providing examples of activities that are considered to be part of the seizure of evidence. One example which is included in the definition is the authorization to activate the suspect’s computer system.

(17) Internet Service Provider

In lieu of providing a single definition of “Internet Service Provider” the Act differentiates between the types of service providers.

(18) Traffic Data

The interception of “traffic data” is an important investigation process, thus, the Act provides 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 objects of seizure. While the interpretation of the term is left to national courts the Act provides 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 it was 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 Act 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 sections 4-15 provide a definition of the minimum standards and therefore allows for more extensive criminalisation should the country so desire.

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 Act 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 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, e.g. 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, is reflecting the fact, that the integrity of a computer system cannot only be violated by entering a computer system without right, but also by remaining in the computer system after the authorisation has expired. There is no similar provision contained in either the Commonwealth Model Law of the Council of Europe Convention on Cybercrime. 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 “nonpublic”, 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 Act ensures that a comprehensive approach is undertaken, especially as older computers generate electromagnetic emissions during their operation. Such emissions which are not covered by the term data within the Act needed to be specifically criminalised.

Section 6 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 the criminal law 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 which makes it unprocessable with regard to its intended use. This act requires that the data was useful or effective before such interference.

“No 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 host 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 which 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 it was 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 tests shall not be criminalised.

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

Two different cases are mentioned in subsection 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 on 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 additional special intent that the device is used for the purpose of committing any of the offences established in part II.

Subsection 2 contains a legal presumption that a suspect who 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 of no consequence whether they are directly readable and/or intelligible. The provision does not only refer 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 11 requires, 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 to 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 that 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.

Section 11 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 Act, 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 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 country may or may not 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 Act.

The term “transfer” covers data transmission processes from one computer to another computer system. This is relevant if databases with identity-related information, which 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 Act.

Section 15 requires that the offender carries out the offences intentionally and without lawful excuse or justification. Therefore authorized computer testing shall not be criminalized.

Section 16: Disclosure of Details of and Investigation

Confidentiality of investigations can be of 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 Assist

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 a provision criminalising harassment utilizing means of electronic communication has been included in the Act. The criminalization requires that the offender initiated an electronic communication. An electronic communication is for example initiated if the offender is sending out an email 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.

**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 seizure 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 and applies to stored computer data. If such warrant is issued it authorises law enforcement authorities to not only 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 techniques that may be used to search or access a computer system has not been specified in the Act. 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. 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 Section 3. 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 indispensable 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. As such an obligation on the relevant persons possessing knowledge of the functioning of a computer system or measures applied to protect computer data therein, has been created by the Act. Such assistance is however limited to that which is reasonably required. Section 21 sets out five (5) areas of assistance. However, it is 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 process in Section 22 (a) which compels a person in its territory to provide specified stored computer data, has been included. 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, requests are limited to those where information is reasonably 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. 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 or 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) a process which enables law enforcement agencies to order the preservation of such data when necessary has been established.

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. If the order for expedited preservation is not in due time followed by either an order for extension of the period, or 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 section enables any police officer to order the expedited preservation. This is in 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 judge.

**Section 24: Partial Disclosure**

Although the drafters of the model legislative text in principle agreed to a strict distinction between the authorisation to order the preservation of data, (which can be given by any police officer), and the order to transmit the data (which requires an order from a judge), they highlighted 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**

Monitoring the traffic data generated during the use of Internet services enables investigators to identify the IP address of an offender and they 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.

The country may in the exercise of its discretion decide not to implement Section 25.

**Section 26: Interception of Content Data**

In some cases the collection of traffic data is not sufficient 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. A provision enabling the interception of data communication has therefore been included. 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; Section 26(b) enables law enforcement authorities to carry out the interception. The country may, however, decide not to implement Section 26.

Section 27: Forensic Software

During the discussion within the working group the drafters of the model legislative text, decided to include a provision authorising investigators to utilize remote forensic software to collect relevant evidence. This process which is very intrusive, could potentially interfere with fundamental rights of the suspect, thus a number of restrictions have been included. Firstly, the use of such software requires that evidence cannot be collected by applying other processes. Secondly, an order by a judge or magistrate is required. Thirdly the application needs to contain specified information (Section 27(1)(a)-(d). In addition the authorised acts are limited by both paragraph 1 and 2. The country may implement further restrictions by limiting the application of the instrument to crimes contained in a list Section 27(7) it may choose not to implement the section at all.

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 as to whether there is an obligation to monitor activities and, whether 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 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 liability of hosting providers have been limited in this Act. 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” in general mean in less than 24 hours.
Section 30(1)(b) provides that as long as the hosting provider has no actual knowledge of illegal activities or illegal content stored on his servers, he is not liable. If information is brought to the attention of a provider, such information must be concrete and specific enough to enable the provider 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 Ecommerce directive, that established liability if the hosting provider does not remove illegal content after having information about its existence, the Act leaves this decision to competent public authorities. As such the 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, but to popular Internet Services like the auction platforms offer hosting services as well. The country may decide to implement a hotline service where illegal content can be reported, depending on the availability of resources.

As the removal of illegal content might, despite the illegal nature of the content interfere with the contractual obligations of the provider with regard to its customers, an exemption has been provided in Section 30(3) regarding 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. Given the economic importance of caching, the provider is exempted from the liability for automatic temporary storage if the conditions defined by Section 31 have been complied with.

**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 liability of hyperlink providers, is regulated 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 providers, the liability of search engines is regulated in accordance with the liability of access provider (Section 29).
Annex 3

Report on
Proposed Cybercrime Policy
Grenada

Section I: Introduction

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

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

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

The Government is aware that the world has become a global village in which different sectors of the economy are very closely interrelated and interconnected, as a result of which, these priority areas are affected by information society issues, which include the need to build the confidence of both consumers and investors in the use of ICTs and the need for ensuring the security of the ICT environment, both of which are prerequisites for the development of an information society.

It has, however, recognised that ICT as an enabling sector is not without its own peculiar challenges, the most serious of these being the challenges presented by cybercrime. As such it has embarked on the development of a legal framework to regulate and facilitate all forms of electronic interaction.

The potential for increase in the frequency and severity of crimes committed with the use of information technology is a very real possibility in light of the increasing dependency on the availability of networks and computer systems as well as the increasing numbers of internet users. This presents serious concerns globally as it affects both the developing and developed world. Consequently, the ability to combat cybercrime is essential to both developed and developing countries.

Further, the internet has become a global market place which promotes e-commerce and enables companies, small and medium sized enterprises and sole traders alike, to offer their products and services worldwide. As the

---

23 Page 12 of 2006-2010 Strategy and Action Plan
24 International Telecommunication Union (ITU), WSIS Outcome Documents, December 2005, p.10
integration of network services, such as e-mail, e-banking and communication through social networks continue to increase in popularity, so too, does the exposure to and risks of cybercrime attacks increase.

In order to protect such users, therefore, it is imperative that countries have the ability to respond quickly and effectively when such services are attacked or otherwise abused.

The necessity of being able to investigate and identify perpetrators of cybercrime as well as the ability to gather digital evidence and conduct successful prosecutions of such perpetrators transcends consumer protection.

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

1.2 Policy on Cybercrime

The Government is aware of the many corollary challenges created by the very benefits derived from an ICT knowledge based society and economy. The potential for increased criminal activity, increased difficulties in detecting crime and a change in the methods used as well as the types of crime committed, are all very real challenges which will be faced and must be effectively dealt with.

The Government has both the responsibility and the power to formulate the relevant policies, to develop the requisite legislative and regulatory frameworks and to enact relevant and effective legislation/law to combat cybercrime, thereby fostering confidence and trust in the use of ICTs, which will aid in the maintenance of national and ultimately, international security and stability, as well as the maximizing of benefits which can be derived from a knowledge based economy and society.

The Government which is also committed to promoting public confidence in the use of ICTs for conducting business of all types and at all levels (both public sector such as e-government, the private sector and civil society), as well as promoting the confidence of both internal and external investors, has recognized the need for the development of a new ICT specific legislative framework and infrastructure. As such it has engaged Stage 2 of the HIPCAR Project\(^ {26}\) to develop relevant policies and legislation in the areas of cybercrime, interception of communications and electronic evidence based on the HIPCAR Model Policy Guidelines and Legislative Texts, which have been greatly influenced by both international and regional best practices, and which were prepared under Stage 1 of the project with the assistance of stakeholders from Grenada and the wider Caribbean region. These three areas are the foundation areas required for the building of a knowledge based society and economy, the nucleus of which is the use of ICTs.

1.3 Purpose of the Policy

The purpose of this proposed Policy is to provide a guiding structure for the Government to develop and implement cybercrime legislation, necessary in the fight against cybercrime.

This document, therefore, sets out the policy which guides the development of the proposed Bill on Computer Crime\(^ {27}\) and Cybercrime. Both the Policy and the Bill are based on the Model Policy Guidelines and Legislative Text on Cybercrime, developed under Stage 1 of the HIPCAR Project.

---

\(^{26}\) The full title of the HIPCAR Project- funded by the European Union and the International Telecommunication Union (ITU) and implemented by ITU in collaboration with CTU- is: “Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, legislation and Regulatory Procedures.” HIPCAR is part of a global ITU-EC project encompassing Sub-Saharan Africa, the Caribbean and the Pacific Islands (ACP) supported by and with funding from the European Union (see http://www.itu.int/ITU-D/projects/ITU_EC/hipcar/index.html)

\(^{27}\) Computer crimes are those crimes committed against a computer or computer system and includes offences such as illegal access, illegal data interference, illegal system interference and data espionage.
The main aim of the Bill is to introduce and facilitate the harmonization of cybercrime legislation in Grenada with that of the regional and international communities, by ensuring it conforms to the HIPCAR Model Policy Guidelines and Legislative Texts and international and regional standards and best practices.

**Section II: Background**

**2.1 Existing Cybercrime Policy**

In its 2006-2010 ICT Strategy and Action Plan, part of the Government’s stated mission is to put ICTs at the center of the country’s social and economic development. It intends to do so by creating an enabling environment for the purpose of attracting local and foreign investors through appropriate policies and legislation.

As Grenada currently has no formal policy directly addressing cybercrime and no effective legislative framework specifically geared at combating cybercrime, the Government has taken the initiative to engage Stage two of the HIPCAR Project to develop a much needed policy on cybercrime. the Government recognizes that a formal policy on cybercrime is an essential tool in ensuring the creation of a relevant and effective legislative framework to safeguard the interests of the citizens and investors alike; as well as to promote their confidence and trust in the use of ICTs in transacting business of all types and at all levels.

The focus of the proposed policy is to lay the foundation for the establishment of effective legislation to combat cybercrime, as such the Government supports the following policy objectives, namely the development of:

1. Legislation, which criminalizes the more common and frequently occurring cybercrimes;
2. Technology neutral legislation enabling its applicability to technological advancements, without the need for constant amendments;
3. Legislation which will readily facilitate regional and international cooperation in the fight against cybercrime.

In this regard, the Model Policy Guidelines on Cybercrime, developed under Stage 1 of the HIPCAR Project are important building blocks upon which the policy on cybercrime can be fashioned to meet the requirements of Grenada.

This proposed policy, therefore, is based on and strongly reflects the key principles set down in the Model Policy Guidelines on Cybercrime.

**2.2 What is Cybercrime?**

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

Cybercrime may be described as any crime committed utilizing computers, computer networks and the internet. It is invariably considered as falling into two main categories, namely, old offences committed with the use of new technologies, for example the use of devices such as smart phones and networked computers, to commit

---

28 See page 12 of the 2006-2010 ICT Strategy and Action Plan
traditional crimes such as fraud, identity theft and money laundering; and new technology used to commit new ICT based offences such as data espionage, interfering with a computer system and illegal data interference.

2.3 The Nature of Cybercrime

By its very nature cybercrime poses particular challenges to existing criminal law and equally to traditional methods of law enforcement. The online environment is a peculiar environment in that cybercriminals can operate globally and from any place in the world; they are no longer restricted by geographical and jurisdictional boundaries/limitations.

Traditional law enforcement therefore, faces the challenges of scale and volume of the crimes perpetrated as well as the technical complexities of identifying not only the perpetrator/s but sometimes also their location.

The internet, sometimes referred to as the ‘criminal’s playground’, provides an excellent cover and conduit for the execution of almost every crime conceivable. Phishing e-mails, SPAM and malicious software can be distributed unlawfully to virtually millions of person located in jurisdictionally and geographically separate countries worldwide, while peer to peer networking enables the proliferation of mega volumes of illegal images.

This proposed policy and the resulting proposed Cybercrime Bill provide a much needed and effective framework for combating cybercrime in Grenada.

2.4 Legislative Approach

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

The proposed Bill seeks to legislate specifically against computer crimes and cybercrimes. It criminalizes certain types of behaviours and acts such as illegally accessing and remaining logged into a computer system without lawful excuse or justification, obstructing, interrupting or interfering with the lawful use of computer data and disclosing details of a cybercrime investigation. None of these types of behaviours or acts are currently legislated against by existing legislation in Grenada.

In light of the Government’s mission and vision as stated in the 2006-2010 Strategy and Action Plan the proposed Policy and Bill on cybercrime are necessary elements in creating, as far as possible, a secure and trusted environment in which to transact all types of business, as they provide the requisite infrastructure for combating cybercrime and promoting the confidence of consumers and investors in the security of transacting online.

2.5 Linkage to Other Legislation

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

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

This policy and the resulting proposed cybercrime bill draws upon and are influenced by these sources.

Both the policy and the bill will directly affect legislation and or legal practices relating to Grenada’s Criminal Code, the Proceeds of Crime Act, the Telecommunications Act, the Interception of Communications Act and the Evidence Act.

They will also have some impact on laws pertaining to banking and to data protection.

Section III: Policy Objectives

3.1 Complementing the National Strategy and Action Plan

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

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

The policy provides that legislation should criminalize certain types of activities and behaviours which are presently not criminalized in Grenada. Examples include interfering with computer systems, intentional and illegal computer related fraud and the intentional and illegal production sale and related acts, regarding child pornography.

It also requires effective procedural instruments enabling competent authorities to investigate cybercrimes and also to provide for transnational cooperation in investigations.

3.2 Objectives of the Proposed Policy on Cybercrime

The basic objectives of the proposed Policy on Cybercrime are as follows:

- To guide the development of an effective cybercrime bill, which complements an ICT knowledge-based society and economy; and

- To promote and enhance the trust and confidence of consumers of online services, by ensuring the resulting Bill provides relevant provisions enabling the detection and effective investigation of cybercrime, the prosecution of cybercriminals and penalties commensurate with the effects of the crimes perpetrated on the victims.

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

---


32 Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int

Grenada 98
Section IV: Key Principles

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

4.1 Establishment of Common Interpretations for Key Terms

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

4.2 Development of Substantive Criminal Law

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

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

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

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

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

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

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

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

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

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

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

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

4.4 Development of Instruments for Transnational Cooperation in Cybercrime Investigations

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

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

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


International Telecommunication Union (ITU), WSIS Outcome Documents, Geneva, Switzerland, 2005


Council of Europe Convention on Cybercrime (CETS No. 185), available at URL: http://conventions.coe.int
### Annex 4

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

Co-organized with the Government of Grenada and the ITU/EU-funded HIPCAR Project

National Stadium, St. George’s, Grenada, 15-16 February 2012

<table>
<thead>
<tr>
<th>ORGANIZATION</th>
<th>LAST NAME</th>
<th>FIRST NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Afi Ventour &amp; Co</td>
<td>ROBERTS</td>
<td>Vincent</td>
</tr>
<tr>
<td>Caribbean Knowledge and Learning Network (CKLN)</td>
<td>VENTOUR-DE VEGA</td>
<td>Afi</td>
</tr>
<tr>
<td>Corporate Affairs and Intellectual Property</td>
<td>BAILEY</td>
<td>Juan</td>
</tr>
<tr>
<td>Customs Department</td>
<td>HENRY</td>
<td>Annette</td>
</tr>
<tr>
<td>Department of Public Prosecution</td>
<td>MARSHALL</td>
<td>Lindonna</td>
</tr>
<tr>
<td>DIGICEL</td>
<td>GREENIDGE</td>
<td>Crisan</td>
</tr>
<tr>
<td>Division of Cooperatives</td>
<td>ALLEYNE</td>
<td>Nadia</td>
</tr>
<tr>
<td>Economic Partnership Agreement (EPA) Implementation Unit</td>
<td>SLINGER</td>
<td>Carolyn</td>
</tr>
<tr>
<td>FLOW</td>
<td>GARRAWY</td>
<td>Nicole</td>
</tr>
<tr>
<td>FLOW Grenada Ltd.</td>
<td>MCINTOSH</td>
<td>Brent</td>
</tr>
<tr>
<td>FLOW Grenada Ltd.</td>
<td>BURKE</td>
<td>Edmund</td>
</tr>
<tr>
<td>FLOW Grenada Ltd.</td>
<td>LAWTON</td>
<td>Opal</td>
</tr>
<tr>
<td>FLOW Grenada Ltd.</td>
<td>PURCELL</td>
<td>Gail</td>
</tr>
<tr>
<td>Grenada Broadcast</td>
<td>GRANT</td>
<td>George</td>
</tr>
<tr>
<td>Grenada Co-operative Credit Union League</td>
<td>MOSES</td>
<td>Aaron</td>
</tr>
<tr>
<td>Grenada Industrial Development Corporation</td>
<td>VICTOR</td>
<td>Kent</td>
</tr>
<tr>
<td>Grenada National EPA Implementation (EPA) Unit</td>
<td>JOHN</td>
<td>Desmond</td>
</tr>
<tr>
<td>Grenada Postal Corporation</td>
<td>SYLVESTER</td>
<td>Ruben</td>
</tr>
<tr>
<td>Inland Revenue Department</td>
<td>LEWIS</td>
<td>Nelson</td>
</tr>
<tr>
<td>LIME</td>
<td>LANGAIGNE</td>
<td>Glendon</td>
</tr>
<tr>
<td>LIME</td>
<td>NOEL</td>
<td>Cecil</td>
</tr>
<tr>
<td>LIME</td>
<td>PITT</td>
<td>James</td>
</tr>
<tr>
<td>LIME</td>
<td>STEELE</td>
<td>Angus</td>
</tr>
<tr>
<td>Organization</td>
<td>Name</td>
<td>Title</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>---------</td>
<td>--------</td>
</tr>
<tr>
<td>Media Workers Association of Grenada</td>
<td>TITUS</td>
<td>Rawle</td>
</tr>
<tr>
<td>Ministry of Education</td>
<td>NURSE</td>
<td>Eric</td>
</tr>
<tr>
<td>Ministry of Finance</td>
<td>BURKE</td>
<td>Nazim</td>
</tr>
<tr>
<td>Ministry of ICT</td>
<td>SIMON</td>
<td>Loretta</td>
</tr>
<tr>
<td>Ministry of Legal Affairs</td>
<td>BAISDEN</td>
<td>Ayesha</td>
</tr>
<tr>
<td>Ministry of the Environment</td>
<td>CHARLTON</td>
<td>Henry</td>
</tr>
<tr>
<td>Ministry of Works</td>
<td>CLARKE</td>
<td>Dennis</td>
</tr>
<tr>
<td>National Insurance Scheme</td>
<td>NOEL</td>
<td>Dwane</td>
</tr>
<tr>
<td>National Telecommunications Regulatory Commission (NTRC)</td>
<td>FERGUSON</td>
<td>Ruggles</td>
</tr>
<tr>
<td>National Telecommunications Regulatory Commission (NTRC)</td>
<td>FERGUSON</td>
<td>Aldwyn</td>
</tr>
<tr>
<td>Prime Minister’s Office, St. Vincent and the Grenadines</td>
<td>THOMSPON</td>
<td>Jerrol</td>
</tr>
<tr>
<td>Procurement Unit</td>
<td>VICTOR</td>
<td>Terrence</td>
</tr>
<tr>
<td>Royal Grenada Police Force</td>
<td>DICKSON</td>
<td>Simon</td>
</tr>
<tr>
<td>Royal Grenada Police Force</td>
<td>GREENIDGE</td>
<td>Teron</td>
</tr>
<tr>
<td>Royal Grenada Police Force</td>
<td>NOEL</td>
<td>Franchesca</td>
</tr>
</tbody>
</table>
## Annex 5

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

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

<table>
<thead>
<tr>
<th>LAST NAME</th>
<th>FIRST NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>BAISDEN</td>
<td>Ayesha</td>
</tr>
<tr>
<td>BAKER</td>
<td>Wynette</td>
</tr>
<tr>
<td>BAPTISTE</td>
<td>Maureen</td>
</tr>
<tr>
<td>BOWEN</td>
<td>Christine</td>
</tr>
<tr>
<td>FOSTER</td>
<td>Francis</td>
</tr>
<tr>
<td>GOODING-De SOUZA</td>
<td>Camille</td>
</tr>
<tr>
<td>LASHLEY-BYER</td>
<td>Nicola</td>
</tr>
<tr>
<td>MARRAST-VICTOR</td>
<td>Kinna</td>
</tr>
<tr>
<td>OLOWU</td>
<td>Adebayo</td>
</tr>
</tbody>
</table>
Annex 6

Participants at Second Stakeholder Consultation/Validation Workshop on Cybercrime, e-Evidence and Interception of Communications
Co-organized with the Government of Grenada and the ITU/EU-funded HIPCAR Project
National Stadium, St. George’s, Grenada, 28 March 2012

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