

LAW AND TECHNOLOGY WORKSHOP FOR THE CARIBBEAN

**Terra Nova Hotel, Kingston, Jamaica
3-7 November 2003**

REPORT

Organised by the

Legal and Constitutional Affairs Division
Commonwealth Secretariat

in collaboration with the

Governance and Institutional Development Division
Commonwealth Secretariat

Legal and Constitutional Affairs Division
Commonwealth Secretariat
Marlborough House, Pall Mall
London SW1Y 5HX
United Kingdom

January 2004

CONTENTS

INTRODUCTION	Page 1
OPENING	Page 2
MEMORANDA OF PRESENTATIONS AND DISCUSSIONS	Pages 3 – 12
❖ Presentation By Mr Rogers W’O Okot-Uma, Chief Programme Officer (GIDD) - “Making the Transition to a Cyberlaw Capacity for eGovernance: Technology Perspective”	Page 4
❖ Model bill on electronic Evidence – Overview by Mr Jeff Cumberbatch, Deputy Dean, Faculty of Law – UWI	Pages 5 - 6
❖ Model Bill On Electronic Transactions – Overview by Mr Jeff Cumberbatch, Deputy Dean, Faculty of Law – UWI	Pages 7 – 8
❖ Overview by Dr. Emmanuel Awuku Privacy Freedom of Information	Pages 9 – 10 Page 9 Page 10
❖ Overview by Ms. Aruna Narain, LCAD and Ms Lucie Angers, Department of Justice, Canada	Pages 11 – 12
CLOSING	Page 12
CONCLUSIONS AND RECOMMENDATIONS	Pages 13 - 23
ANNEXES	
Annex 1 – Commonwealth Model Laws (see model laws at www.thecommonwealth.org/law)	27
❖ Annex 1.1 – Electronic Evidence Model Law	29
❖ Annex 1.2 – Electronic Transactions Model Law	33
❖ Annex 1.3 – Freedom of Information Model Law	43
❖ Annex 1.4 – Privacy Model Law	61
❖ Annex 1.5 – Computer and Computer Related Crimes Model Law	77

Annex 2 – Papers Presented:	89
❖ Annex 2.1 “Making the Transition to Cyberlaw Capacity for eGovernance: Technology Perspectives” - Rogers W’O Okot Uma	91
❖ Annex 2.2 “Electronic Evidence – The Caribbean” – Mr. Jeff Cumberbatch	97
❖ Annex 2.3 “The Commonwealth Model Law on Electronic Transactions” – Mr. Jeff Cumberbatch	101
❖ Annex 2.4 “The Development of Privacy Legislation” – Dr. Emmanuel Opoku Awuku	105
❖ Annex 2.5 “The Development of Legislation on Freedom of Information” – Dr. Emmanuel Opoku Awuku	111
❖ Annex 2.6 “The Commonwealth Computer and Computer Related Crimes Act: An Overview” – Ms. Lucie Angers	117
Annex 3 – Country Reports of Participants	121
❖ Annex 3.1 – The Bahamas	123
❖ Annex 3.2 – Barbados	127
❖ Annex 3.3 – Belize	129
❖ Annex 3.4 – Dominica	137
❖ Annex 3.5 – Guyana	141
❖ Annex 3.6 – Jamaica	143
❖ Annex 3.7 – St. Lucia	147
❖ Annex 3.8 – St. Vincent and the Grenadines	151
Annex 4 – List of Participants	153
Annex 5 – Agenda	159
Annex 6 – Electronic Communications and Transactions Act of South Africa	163

INTRODUCTION

In 1999 Commonwealth Law Ministers at their meeting in Trinidad and Tobago mandated the Commonwealth Secretariat to look at the legal implications arising from the use of technology and assist Member Countries in taking full advantage of the opportunities presented by technological developments.

The Secretariat convened several expert groups and prepared drafting instructions from their deliberations. Model laws (**Annex 1**) dealing with technology were specifically drafted on the following:

- Electronic Transactions;
- Electronic Evidence;
- Freedom of Information;
- Privacy; and
- Computer and Computer Related Crimes

These model laws were submitted to Law Ministers for consideration at their meeting in 2002 in St Vincent & the Grenadines. They commended the laws and asked the Secretariat to continue to work with senior officials in these areas to ensure that the laws remain current and reflective of the interests of Member Countries, particularly small and developing states.

It is in light of these mandates, that the **Legal and Constitutional Affairs Division (LCAD)** in collaboration with the **Governance and Institutional Development Division (GIDD)** of the Secretariat convened a regional workshop for the Caribbean. This is the first of a series of workshops which seek to promote the adoption/adaptation of these laws. In conducting these workshops, the Secretariat recognises that individual countries are at different stages of development. The model laws therefore provide flexibility for countries to adapt to suit their circumstances. The Secretariat and LCAD further recognise that harmonised laws by regional Member Countries will also greatly facilitate the operation of their regional arrangements. Part of the Secretariat's role is to assist Member Countries in capacity-building and developing these model laws go towards fulfilling that objective. The participants welcomed the model laws and commended them for use.

The papers presented at the workshop were insightful and thought provoking - see **Annex 2**. Participants also made presentations on the position within individual countries in relation to the status of their respective legislative frameworks for an eGovernance regime - see **Annex 3**

The countries represented were: The Bahamas, Barbados, Belize, Dominica, Grenada, Guyana, Jamaica, St Kitts & Nevis, St. Lucia, St Vincent, Trinidad & Tobago. The

Caribbean Community Secretariat (CARICOM) was also represented. **(See List of Participants at Annex 4).**

OPENING

The meeting was opened by the Attorney General of Jamaica, the Hon A J Nicholson. He welcomed the participants and thanked the Secretariat for initiating the idea of developing the model laws, securing Commonwealth Law Ministers' mandate and bringing the idea to fruition. He reiterated the importance of technology and the potential it offers for development. He noted that such impact on economic development comes in positive as well as negative forms. The Attorney General advised that whilst the positive aspect is reflected in the ease with which business could be conducted electronically, the negative aspect is demonstrated by the rise in Computer and Computer-Related Crimes.

The Attorney-General referred to the terrorist threat faced by the Caribbean region, and particularly drew attention to drug trafficking and money laundering. He stressed the significance of having relevant laws in place if the region is to be able to compete effectively in an increasingly global age. This, he reiterated as being even more important given that the Caribbean economy is becoming service based thus requiring the necessary infrastructures to support development and strengthen the economic foundation of the region.

On the issue of the regulation of electronic transactions, the Hon. Attorney General agreed with the view that they should be regulated, but cautioned against the extent to which such regulation must go. He charged the meeting with the responsibility of finding a balance.

The Hon. Attorney General acknowledged that it was impossible to build expertise out of a one week workshop, but drew attention to the advantages which can be realized from one. He emphasized that this included the opportunity to network with colleagues in other countries, maintaining contact and keeping up with developments in other jurisdictions. He expressed confidence in the ability of delegates to strengthen the legal environment in the region and wished them a productive meeting.

The Secretariat team was led by Ms Thompson-Barrow, Head of the Law and Development Section, LCAD, who chaired the meeting.

The meeting considered and adopted the draft agenda. **(Annex 5)**

MEMORANDA OF PRESENTATIONS AND DISCUSSIONS

**PRESENTATION BY MR ROGERS W’O OKOT-UMA, CHIEF
PROGRAMME OFFICER (GIDD)**

**“Making the Transition to a Cyberlaw Capacity for eGovernance:
Technology Perspective”**

Mr Rogers W’O Okot-Uma opened the workshop with this presentation. He reflected on the manner in which the concept and practice of good governance begun and had evolved over the last fifteen years. He noted that the starting point for the Commonwealth was the affirmation of its commitment to good governance and that this is enshrined in its 1991 Harare Declaration which advocates good governance as one of its fundamental values. He remarked that Electronic Governance must be incorporated into the effort to achieve good governance, defining Electronic Governance as the efforts of governments to deploy Information and Communications Technology (ICT) to enable:

- (i) the process of administration of government and the process of delivery of government services to the public (known as *eGovernment*);
- (ii) the process of government-citizen consultation, aimed at empowerment of the citizen and civil society (known as *eDemocracy*); and
- (iii) the process of government-business transactions, government-government partnerships and collaboration (known as *eBusiness*).

He advised that the implementation of *eGovernance* usually takes place in an evolutionary progression through a number of levels. At the lowest level, is the internalization and informing factors of enablement of trustworthy computing which include the necessity for integrity and availability of data. At the next tier is the interaction of additional factors which include the promotion of the need for privacy, identity, data, communication and confidentiality. At a further stage even beyond that point, (namely transacting, integrating and transforming) is the promotion of trust and confidence which become significant. Rogers believes that if there is to be trust and confidence in the deployment of a full *eGovernance* system in a national jurisdiction, three elements are essential, which would enable the citizenry to live and work in the wired world. These are:

- (i) a trusted business environment;
- (ii) a suitable legal framework; and
- (iii) valid laws of evidence.

With these rousing thoughts, he commended the Commonwealth model laws to Member Countries.

MODEL BILL ON ELECTRONIC EVIDENCE

Overview by Mr Jeff Cumberbatch, Deputy Dean, Faculty of Law - UWI

Mr Cumberbatch commented on the difficulty he experienced in accessing all the laws of Member Countries. He encouraged participants to ensure that when laws are enacted, copies are sent to the library of the University of the West Indies (UWI) or where such laws are placed on the internet, government officials should endeavour to notify UWI so that it is kept aware of legal developments in the CARICOM Member Countries.

In addressing the model law, he praised its brevity, simplicity, flexibility and clarity of language and encouraged its use by Member Countries. As well as meeting its overall objectives, he was satisfied that the model law fulfilled its basic objective – the removal of the objection to have an electronic record admitted by a court on the sole basis that the record is electronic. He pointed out the provisions of the model bill which go to the admissibility of such electronic records including the presumption of the integrity of the electronic system, thus bypassing the need to prove technical details.

Mr Cumberbatch also drew attention to the options available to countries to either let the e-Evidence model law stand alone or as an amendment to existing evidence laws.

In response to the presentation, the meeting noted that within the definition of the model law a new concept appears to be introduced by distinguishing between “computer record” and “computer record system”. The explanation to this was that “computer record system” is intended to cover matters such as network, telecom etc. It was pointed out that another name is now evolving – “information system” – which is meant to be even more inclusive, covering wider areas.

Participants questioned the possibility for countries to move away from the model law and apply standards which are reflective of local culture and circumstances. There were doubts expressed on this as it was felt that if a jurisdiction is to be able to attract foreign investors, genuinely compete internationally and experience real economic development, then the standards applied must be acceptable to the international community. It was recalled that in drafting each of the model laws international documents had been considered such as the UNCITRAL model law and the Council of Europe’s convention on cyber-crime. All the model laws therefore set internationally acceptable standards.

In light of the discussions the meeting recognized that the imminent Caribbean Single Market and Economy would be best served with harmonized laws of its Members.

Thought was given to CARICOM Member Countries enacting a comprehensive legislation to deal with all matters arising under electronic governance. The meeting took note of South Africa's approach through its Electronic Communications & Transactions Act - **(See Annex 6)**. Copies of the legislation were distributed and it was highly praised both for its comprehensive nature and also for its bold innovation of embodying law and policy in one document. This unique piece of legislation from South Africa was therefore recommended as another model to study, as well as Singapore's and India's laws which were considered.

The meeting acknowledged that not many countries had taken a comprehensive approach towards the development of e-governance. It noted the lack of cohesion between several departments/ministries within individual countries which have responsibility for different areas of e-governance. The meeting recommended that countries should ensure that relevant departments work together and adopt an all embracing approach, thus ensuring the development of strong and consistent policy and law.

The meeting acknowledged the importance of noting the directions in which countries are headed and how best to move with the Commonwealth model laws along similar paths. It was accepted that this might present some difficulties given that individual Member Countries were at different stages of implementation. Whilst some had already enacted all the laws, others have partial enactments. For those who are yet to enact and those still in the process of doing so, there exists the opportunity, as a result of the knowledge gained from the present workshop, to make appropriate assessment before embarking on enactment. In this regard, the meeting decided that both the Commonwealth and CARICOM Secretariats should be requested to continue to render assistance to the region in general and to designated countries where the needs are specific.

There was concern on the impact these enactments might have given the lack of uniformity of the laws of Member Countries. Mr Duke Pollard, representing the CARICOM Secretariat explained that the focus should not be on uniformity but on harmonisation of laws. He confirmed that there are structures in place which seek to harmonise the laws of CARICOM Member Countries so that cross-border interactions are made easy and enforcement problems are avoided. Harmonisation, it was noted, will also enable a proper functioning of the Caribbean Court of Justice. There was general concurrence with this view and the meeting recommended that efforts should be made to harmonise the laws of the region.

MODEL BILL ON ELECTRONIC TRANSACTIONS

Overview by Mr Jeff Cumberbatch, Deputy Dean, Faculty of Law - UWI

Mr Cumberbatch noted the objectives of the model law which are listed in section 3 and pointed out the comprehensive nature of these objectives. He also made comparisons with other laws – from the British Virgin Islands, Barbados and Bermuda which he had considered in the process of reviewing the Commonwealth model law.

He lauded the features of the model law such as the concept of opting in or out which gives parties to a transaction a choice to determine whether or not to use electronic means to conduct such transactions. He noted the expressly excluded documentary list relating to the process of electronic transactions and the flexibility available to governments to extend or reduce the list through regulations.

Mr Cumberbatch pointed out that under the Commonwealth model law, the use of electronic transactions is not mandatory. Transacting parties must consent to such use, even though inference could be drawn in determining whether or not consent was given. He touched on automated contracts and observed that the legislation of the countries he considered (i.e. BVI, Bermuda and Barbados) did not provide for this, but that the South African law makes necessary provisions. The Commonwealth model law also provides for this feature in section 19. Section 20 takes it even further to allow for remedy where automated functions are used and error occurs. When the issue of what constitutes prompt notification arose under s.20(c), there was wide support for the view that the common law position would apply (i.e. reasonable time to notify the other party of the error).

Under section 24, a person purchasing items on-line is given protection by the requirement for the seller to have certain basic information available on-line so that anyone accessing the website could download such information. Mr Cumberbatch asked participants to consider recommending that countries should enact separate legislation on consumer protection. This is because section 24 only protects consumers conducting transactions on-line. It was felt that one law protecting all consumers, regardless of the method of purchase, would suffice. Outside the model law, it was noted that some laws provide for the liability of Internet Service Providers (ISPs).

Mr Cumberbatch felt that there could be potential conflict arising from section 5 where the model law purports to bind the Crown, Government or State (whichever one applies). He noted that this tends to conflict with the section 17 which gives parties the option of whether or not to enter into electronic transactions. The Chair intervened and clarified that given the philosophical underpinning of an ultimate eGovernance/eGovernment regime; the Crown/State/Government would have to be bound as would its citizenry. He commented on the difficulties presented by the issue of jurisdiction and conflict of laws as regards electronic transactions.

The presentation was followed by discussions among the delegates. There was concern about section 14(4) which states:

“Where a public body consents to receive any information in electronic form, it may specify:

- (a) the manner and format in which the information shall be communicated to it;*
- (b) the type or method of electronic signature required, if any;*
- (c) control processes and procedures to ensure integrity, security and confidentiality of the information;*
- (d) any other attributes for the information that are currently specified for corresponding information on paper.”*

Some delegates wondered about the possibility of individual countries developing their own standards. This view was rejected because it was felt that such approach is likely to create inconsistency and therefore present difficulties. An approach based on common policy was supported whereby countries might determine what to release in terms of access to information while balancing the need for freedom of information with the need to maintain privacy. It was recommended that the CARICOM Secretariat should be charged with the task of developing such standards based on harmonised laws. Such move, the meeting noted, would be compliant with the Treaty of Chaguaramas. The CARICOM delegate further clarified that while the integration process was moving towards a harmonised legislative environment, CARICOM would not have a supranational character, which occurs in other regional movements such as the European Union.

On the issue of effectively tracing where the intended recipient had denied receiving the document, the meeting noted that this would raise the issue of the integrity of the system. If tracing becomes a problem then the system does not have reliability and therefore lacks integrity.

On s.22(2)(a) of the model law, the discussions were similarly focused on the presumption of receipt by an addressee on a “designated” information system. It was clarified that such “designation” would occur in a situation where one party had instructed the other party to send his/her communication in a particular manner (e.g. by email) to that information system.

Finally, some delegates noted the definition section of the model law and felt that this could have been expanded, defining matters such as what constitutes electronic transactions. It was explained that the model law only serves to guide countries in enacting their own laws.

MODEL BILLS ON FREEDOM OF INFORMATION AND PRIVACY

Overview by Dr. Emmanuel Awuku

PRIVACY LEGISLATION

Dr Awuku gave the background to the genesis of the model bills by reflecting on the 1999 endorsement of the Commonwealth Law Ministers in Trinidad and Tobago, of the Commonwealth Freedom of Information Principles, believing the obverse side of the freedom of information coin is the protection of personal privacy. This was therefore the basis for the Secretariat's proposal for the consideration by Commonwealth Senior Law Officials in November 2001 of a model Bill on Privacy.

Dr Awuku then pointed out that some privacy laws make provisions for the establishment of an Independent Privacy Commissioner with a range of functions and powers. Recognising that small and developing countries may not be able to create such an office and may need to rely on courts or tribunals to deal with allegations of damage caused by breach of the privacy law; provisions included in the model bill dealing with the creation of a Privacy Commissioner are on an optional basis.

In greater elucidation and discussion on the office of the Privacy Commissioner, it was confirmed that the appointment of a Privacy and Data commissioner as in the Commonwealth Secretariat's model bill is pursuant to the similar provisions relating to the appointment of a Chief Justice. Appointments of Commissioners and like officials are also conducted by independent autonomous bodies such as the Judicial Services Commission or the Public Service Commissions, thus guarding zealously the independence of the office of the Commissioner. Coupled with these traditional forms of appointment is the new funding style whereby the funds of the Commission are placed as a direct charge on the Consolidated fund, as opposed to parliamentary allocation.

The discussions revealed that not many Caribbean countries have enacted privacy legislation, and for those who already had done so, there was now the thinking of amending their privacy legislation to cover both private and public sector.

Trinidad and Tobago, Barbados and the Bahamas have enacted a Data Protection legislation based on the United Kingdom and Irish model. It was then recommended that in enacting such legislation the public and private sector should be taken into consideration. It was pointed out that in cases where there is no privacy or data protection legislation in place, legislative support is gathered from the constitutions and other principles relating to confidentiality.

It was also recommended that implementation of such legislation must be backed with public education.

FREEDOM OF INFORMATION

It was pointed out that the Commonwealth Secretariat as an inter-governmental organisation is guided by human rights as enshrined in the 1991 Harare Commonwealth Declaration which calls for the promotion of democracy, the rule of law, just and honest government, fundamental rights, including the right to information.

It was on this basis that LCA D decided to pilot work on the subject and place it before the Commonwealth Law Ministers at their Meeting in 1999 in Trinidad and Tobago. The Law Ministers recognised in particular the importance of public access to officials' information, both promoting transparency and accountable governance and encouraging the full participation of citizens in democratic processes. In the same year, the Commonwealth Heads of Government at their meeting in Durban endorsed the Commonwealth Freedom of Information Principles and Guidelines.

The meeting was informed of the few Commonwealth countries which have already enacted legislation on freedom of information or incorporated it in their national constitutional frameworks. However, it was admitted that in most Commonwealth countries the law does not protect this right.

Dr Awuku reinforced the principle that the right to information is an essential element of democratic government - if democracy is to flourish, citizens must be adequately informed about the operations and policies of their government.

The main objective achieved in the Freedom of Information model bill is the provision of the right to information as a basic right as spelt out in international human rights instruments. The key elements of the model law enunciates the object, publication of documents, right of access to information, exempt documents, right to request correction, remedies and appeal, and the establishment of a freedom of information commission.

It was recommended that any countries intending to enact freedom of information in line with Commonwealth Secretariat's model bill must note that adoption such law must be depend on a state's own internal policy consideration and its peculiar national circumstances.

MODEL BILL ON COMPUTER AND COMPUTER RELATED CRIMES

**Overview by Mrs Aruna Narain, LCAD and Ms Lucie Angers, Department of Justice,
Canada**

Mrs Narain stressed the importance of not only enacting relevant legislation but also of constantly reviewing it so as to ensure that it is kept current with respect to emerging technologies and new investigative techniques. She then spoke of the need for a comprehensive range of well-defined offences, sufficiently severe penalties and extraterritorial provisions, and stated that no country should, through inadequate legislative provisions, become a safe haven for cyber-criminals. She laid emphasis on the fact that any legislation on Computer and Computer-Related Crimes should be complemented by effective legislative measures on extradition and mutual legal assistance.

Ms Lucie Angers began her overview of the Model Law on Computer and Computer-Related Crimes by examining the three different ways of committing crimes with a computer-by using the computer as a tool, a storage device or a target. She considered the challenges posed by computer crimes and presented domestic and international solutions, which include the criminalisation of computer-related abuse, the development of international procedural laws for effective investigation and prosecution of cyber-criminals, and the improvement of government-industry cooperation and of international cooperation.

Ms Angers then examined the Model Law on Computer and Computer-Related Crimes in detail, looking at the elements of each of the offences set out at sections 5 to 10 of the Model Law. She went on to consider the provisions setting out the procedural powers at Part III of the Model Law and the definitions at sections 2 and 11 of the Model Law. She also explained other provisions of the Model Law, namely those relating to jurisdiction, evidence, disclosure and liability. Lastly, Ms Angers discussed the pros and cons of enacting legislation on Computer and Computer-Related Crimes either as stand-alone legislation or as an amendment to the Penal Code or general criminal procedural laws.

The main lines of the presentation of Ms Angers are annexed to this report, at **Annex 1**.

Discussion on the model law on Computer and Computer-Related Crimes was lively and related mainly to the procedural powers set out at Part III of the Model Law, especially the provisions regarding search (sections 11 and 12), assistance (section 13) as opposed to production (section 15) and preservation (section 17). The need for reasonable safeguards to be included in the legislative provisions setting out some of these powers was recognised. On the other hand, it was also felt that in view of the need for speed in such investigations, provision should be made for applications to be made for tele-warrants in appropriate cases.

Definitional issues in relation to child pornography (section 10) were also considered. The meeting discussed the criminal liability of Internet Service Providers (ISPs), and was of the view that statutory limitation periods of 6 months in some countries in the region may be too restrictive in view of the complexity of investigations related to computer crimes. Orders for payment of compensation as provided for in the Singaporean legislation and in the law in Trinidad and Tobago were also discussed. Constitutional issues surrounding access to seized computer data and interception of data were debated. The meeting was further of the view that the offence of illegal interception of data (section 8) should be extended to private communications intercepted through public or non-public transmission facilities.

The meeting agreed that necessary legislative provision would have to be made for international cooperation and, in particular, for the making of , and for giving effect to, requests for extradition and mutual assistance relating to Computer and Computer-Related Crimes. The meeting was of the view that the Harare Scheme on Mutual Assistance in Criminal Matters should be amended to provide inter alia for preservation orders and real-time search and tracing of computer data. The need for expeditious execution of requests for extradition and mutual legal assistance was recognised. The meeting supported the idea of joining existing 24/7 networks such as the one set up under the 2001 Convention on Cybercrime.

Finally, the meeting expressed the view that proper enforcement of any legislation relating to Computer and Computer-Related Crimes would require sustained and innovative training of law enforcement officials. Ms Angers informed the meeting of training courses that were run in Canada for law enforcement officials, while Mr Okot-Uma invited countries in the region to seek assistance from the Commonwealth Secretariat through their respective Point of Contact.

The Model Law on Computer and Computer-Related Crimes was commended by the meeting as a useful basis for developing appropriate legislation on the subject.

CLOSING

On the final day of the meeting, Conclusions and Recommendations arising from the meeting were presented and are included here as a part of this Report. Some amendments were made and the document was adopted by the meeting. The meeting commended the success of the workshop and thanked the Secretariat for facilitating the workshop as part of its efforts to assist Member Countries with capacity-building. The meeting was closed by the Attorney General of Jamaica, the Hon A.J. Nicholson who congratulated the delegates for diligently carrying out their task.

CONCLUSIONS

AND

RECOMMENDATIONS

MODEL LAW ON ELECTRONIC EVIDENCE (eEVIDENCE)

1. Computer Record

The meeting observed that within the definition of the model law on Electronic Evidence a new concept appears to have been introduced by distinguishing between “electronic record” and “electronic records system”. The explanation was that “electronic records system” is intended to cover devices including the computer system and associated devices in which data is recorded or stored. It was further elucidated that another name is now evolving which is intended to be even more inclusive than “computer records system”, known as the “information system”. Countries which have not enacted their laws were asked to take note of this and give consideration to its use.

2. Applicable standard

2.1 The issue of applicable standard arose. The meeting considered the possibility of each Member applying its own standard in order to reflect local culture and circumstances. The meeting expressed doubts on this approach. It felt that if a jurisdiction is to be able to attract foreign investors, genuinely compete internationally and experience real economic development, then the standards applied must be that which are acceptable to the international community. The meeting was advised that in drafting each of the model laws international documents had been considered such as the UNCITRAL model law. The meeting was thus cautioned against reducing international standards in national legislation.

2.2 In light of the move of the Caribbean region towards a Caribbean Community (CARICOM) Single Market and Economy, the meeting recognised that such international values would need to be reflected in the laws and policy. As an alternative, it was suggested that a regional standard could be developed, based on harmonised laws of the region. CARICOM was charged with this task.

3. Different Stages in Individual Countries

The meeting acknowledged the importance of noting the directions in which countries are headed and how best to move with the Commonwealth model laws along similar paths. It was that accepted that this might present some difficulties given that individual Member Countries were at different stages of implementation. Whilst some had already enacted all the laws, others have partial enactments. For those who are yet to enact and those still in the process of doing so, there exists the opportunity, as a result of the knowledge gained from the present workshop, to make appropriate assessment before embarking on enactment. In this regard, the meeting decided that both the Commonwealth and CARICOM Secretariats should be requested to continue to render

assistance to the region in general and to particular countries where the needs are specific.

4. Impact on Uniformity/Harmonisation of Laws

Some concern was expressed on the impact of the enactment of the model laws on the Caribbean region given the lack of uniformity of the laws of Member Countries. This disquietude was coupled with the concern articulated by some countries in their relations with third party states who are not Members of CARICOM. An example was given in the case of Belize who is a Member of CARICOM and also a part of the Central American system. The general response was that if the laws of countries were harmonised the concerns expressed would be removed. As regards non-CARICOM states, it was advised that countries should not give special treatment but should endeavour to apply uniformity. The adoption of the Commonwealth model law provides flexibility for Member Countries to do so.

5. Automated Contracts

The meeting considered section 19 of the Commonwealth model law which provides for the use of automated contracts, and section 20 which states the condition under which such transactions will not be regarded as a contract but allows a mistake made during the formation of such contracts to be remedied. It was felt that section 20 may not be adequate to cover errors. The meeting believed that the nature of automated contracts might require the enactment of a separate law and recommended that countries should consider this approach.

MODEL LAW ON ELECTRONIC TRANSACTIONS (eTRANSACTIONS)

6. As part of a general comment on the drafting style of the model law which touches on matters such as whether it could have expanded more on the definition section to include matters relating to the question of what constitutes electronic transactions, it was explained that the model law only serves to guide countries in enacting their own laws. It was therefore accepted that national laws could enlarge the definition section.

7. Consumer Protection (clause 24)

The meeting generally adopted the provisions of the model law. It considered the clause dealing with consumer protection and noted that this only protects consumers conducting transactions electronically such as someone buying on-line. The meeting agreed that this is an area where countries might consider enacting separate legislation on consumer protection. Such legislation should protect all consumers whether or not they are buying electronically. Countries might also consider providing for the liability of Internet Service Providers (ISPs). It was noted that the Commonwealth model laws did not provide for this.

MODEL LAWS ON FREEDOM OF INFORMATION AND PRIVACY

8. Technical Assistance and Capacity Building

8.1 The meeting recognised that the Commonwealth Secretariat operates on a demand-driven basis, therefore where the need is indicated, Member Countries, perhaps in collaboration with CARICOM can seek assistance from the Commonwealth Secretariat in organising national workshops or symposia, making drafting preparations, amendments etc, prior to submission to the relevant Chief Parliamentary Counsel

8.2 The meeting commended countries such as Trinidad and Tobago who had taken steps to provide training for designated Officials under the Freedom of Information Act. This is especially useful in countries with a secrecy culture and consequent reluctance of government officials to provide the public with information. Trinidad & Tobago designates an officer who works with the FOI Unit and has responsibility for coordinating requests and information from the public through various government departments. The meeting commended this approach to Member Countries.

9. Applicability of the Commonwealth Model Law

9.1 It was recommended that countries embarking on enacting these laws in line with Commonwealth Secretariat's model bills must note that whilst such laws can be based on its own internal policy consideration and its peculiar national circumstances, international standards must be reflected.

9.2 For those countries that are yet to enact similar laws and those seeking to amend existing laws, the laws of Trinidad and Tobago and those of Belize were commended for consideration, along with the Commonwealth model law.

9.3 It was recommended that the Commonwealth Secretariat Model Bill on Privacy is good, but it does not cover the private sector and therefore there were consensus that any privacy legislation should cover both the public and private sector.

9.4 The meeting noted that the Commonwealth model law does not have provisions establishing the office of the Information Commissioner and that the office of the Privacy Commissioner in the Commonwealth's Privacy bill is optional. This approach was a recognition of resource constraints which may prevent small and developing jurisdictions from establishing such offices. The alternative recommendation is to assign the functions to an existing office such as that of the Ombudsman or the Human Rights Commissioner or designated body.

9.5 The meeting agreed that the independence of the office of the Commissioner is paramount and there is to be the possibility of the Commissioner successfully carrying out his/her functions. In this regard, the meeting recommended that along with the other

ways in which the independence of that office is measured, such independence must also be reflected in the method of appointment of the Commissioner. The meeting also recommended that the law should specifically state that the office is independent.

10. Encouraging Public Awareness

10.1 The meeting noted that if success is to be achieved in this area, all stakeholders must be involved and public awareness should be encouraged through various media. This would assist governments towards taking a comprehensive approach in the implementation of eGovernance.

10.2 The meeting agreed that freedom of information must also be underpinned by adequate information management systems.

MODEL BILL ON COMPUTER AND COMPUTER RELATED CRIMES

11. Fighting cyber-crime requires a critical examination by States of their criminal legislation and procedures to ensure that there are no safe havens for those committing computer and computer-related crimes. Domestic legislation relating to computer and computer-related crimes may either be included in stand-alone legislation dealing specifically with this issue or in general penal legislation. Further, domestic legislation should be periodically reviewed and kept up to date with respect to evolving technologies and investigative techniques.

12. The Workshop considered the Model Bill on Computer and Computer-Related Crimes and concluded that it formed an excellent basis for the development of effective legislation for fighting such crimes.

13. Substantive offences and penalties:

The meeting recommended that countries should:

- Monitor and identify harmful conduct involving new technologies and enact laws to criminalize all forms of computer-related abuse, including crimes committed against the confidentiality, integrity and availability of computer systems and data, and crimes facilitated through the use of computer systems.
- Ensure that the offence of illegal interception of data is applicable to private communications intercepted either through public or non-public transmission facilities.
- Create sufficiently severe penalties to deter would-be offenders.

14. Procedural powers:

14.1 The meeting recommended that countries should:

- Develop measures to ensure the ability of law enforcement and other criminal justice personnel to effectively investigate and prosecute computer and computer-related crime. Subject to adequate safeguards, include powers to:
 - - Search and seize computer equipment and peripherals, such as hard drives and software;
 - Search and seize data (i.e., copy data) without the necessity to seize the medium upon which it is stored
 - Determine the source or destination of computer communications and telecommunications, both retrospective and prospective
 - Intercept computer communications and telecommunications for the purpose of acquiring their informational content, as well as the related traffic data
 - Require persons to provide assistance that is reasonably required in order to give effect to the above-mentioned powers.
- Harmonize legal and technical standards for the collection and preservation of electronic evidence.
- Ensure, in view of the length and complexity of computer-related investigations, that the prosecution of computer and computer-related crimes is not barred by restrictive statutes of limitation.
- Consolidate and facilitate efforts to combat cyber-crime by inter alia, developing and training in innovative techniques for investigative and prosecutorial personnel.

14.2 Noting the above, the meeting however cautioned against unduly harsh investigative powers and in particular, advised countries to ensure that reasonable safeguards are included in the legislative provisions allowing access to seized computer software. The meeting noted that the investigative powers provided for in the Model Bill may necessitate amendments to the Constitution in some Member Countries.

14.3 The meeting recognized the need for speed in investigating computer and computer-related crime, especially where computer data is likely to be erased. It was therefore recommended that law enforcement personnel should be allowed to seek tele-warrants in order to expedite computer crime-related investigations.

15. International cooperation

The meeting recommended that countries should:

- Where appropriate, ensure in view of the high volatility of computer data, that the legislation provides for or allows expeditious execution of mutual legal assistance and extradition requests with respect to computer and computer-related offences, including expedited means of communication for the transmission and receipt of requests. Grounds for refusal should be limited.
- With respect to mutual legal assistance, provide for mechanisms at the international level equivalent to those provided for use at the domestic level with regard to the investigation of computer and computer-related crimes, including preservation orders, real-time search and tracing of computer data and the non-disclosure of confidential data transmitted pursuant to mutual legal assistance requests.
- With respect to extradition, ensure that computer and computer-related crimes are extraditable offences
- Facilitate international cooperation by making appropriate changes to the Harare Scheme relating to Mutual Assistance in Criminal Matters and ensuring that domestic legislation allow for extradition and mutual legal assistance for all computer and computer-related offences.
- Enact laws or negotiate agreements concerning trans-border search and seizure of computer systems.
- Encourage states to join existing 24/7 networks for ensuring speedy assistance among themselves and the international community
- Encourage technical cooperation through the exchange of information and expertise between and among states

OVERALL CONCLUSIONS AND RECOMMENDATIONS

16. It was agreed that the Commonwealth model laws were timely and should be treated as a working tool, serving as a guide to Commonwealth Member Countries in drafting and enacting their own laws. Their delivery at the workshop was signalled as being a significant contribution towards capacity-building within the CARICOM region, particularly with the emergence of the CARICOM Single Market and Economy. The CARICOM Members readily acknowledged the supreme advantage which a legislatively harmonised regime in the region could bring to the imminent Caribbean Court of Justice.

17. The laws were hailed as being essential to the capacity building of e Governance. The meeting recommended that a useful starting point would be to recognise the significance of good governance which is a priority on the international agenda and remains one of the Commonwealth's fundamental values. The inextricable link of a sound legislative framework towards achieving the requisite level of e Governance was hailed as being imperative to obtain the features of an eGovernance society - *viz*:

- ✦ efficiency in the delivery of government services to the public;
- ✦ allowing the easy flow of information between Government and citizenry;
- ✦ having the ability to prosecute offenders;
- ✦ facilitating the method of conducting transactions; and
- ✦ encouraging transparency and accountability in public institutions

18. The CARICOM Member Countries, at the end of the workshop, would determine to recommend to their governments, whether to enact a comprehensive legislation one on hand or individual but connected pieces of legislation on the other. The meeting felt inclined towards the merit of a composite legislation being more beneficial. In this regard, the South African, Indian and Singapore laws which are all embracing of e Governance issues, were appreciated. In particular, the South African legislation - the Electronic Communications & Transactions Act - was highly commended for its bold initiative in embodying law and policy in one instrument. It was also recommended that countries embarking on enactment might take the South African approach of marrying policy with law.

19. In addressing the question of comprehensively legislating for an eGovernance regime, the meeting discussed the challenges presented in many Member Countries by the lack of cohesion between several departments/ministries which have responsibility

for different areas of eGovernance. This view was also supported by the Commonwealth Secretariat in its experience of visiting Member Countries.

20. On the matter of Member Country request of the Commonwealth Secretariat for technical assistance, the Commonwealth Secretariat reiterated its position of operating on a demand-driven basis. Those Member Countries which are in the process of identifying their needs of the Commonwealth Secretariat, agreed to submit their requirements to the Commonwealth Secretariat in collaboration with CARICOM.

21. For those countries that are yet to enact similar laws and those seeking to amend existing laws, the laws of Trinidad and Tobago and that of Belize were commended for consideration, alongside the Commonwealth model laws.

January 2004

**LEGAL AND CONSTITUTIONAL AFFAIRS DIVISION
THE COMMONWEALTH SECRETARIAT**

ANNEX 3 – COUNTRY REPORTS

ANNEX 3.1

COMMONWEALTH REGIONAL WORKSHOP ON LAW AND TECHNOLOGY

Paper Presented by the Bahamas Delegation

In order to facilitate the country's move to a digital economy, The Bahamas first introduced measures aimed at liberalizing the telecommunications sector. Two significant pieces of legislation were passed in this regard:

- (a) the Public Utilities Commission (Amendment) Act 2000 established the Public Utilities Commission ("PUC") as the independent regulator of telecommunications in The Bahamas from March 2000; and
- (b) the Telecommunications Act which came into force on March 25, 2000, which set the regulatory framework for telecommunications, licensing of telecommunications service providers and the privatization of the government-owned telecommunications company.

The compendium of the 2003 e-commerce legislation which are now enacted as law in The Bahamas are:

- (a) the Electronic Communications and Transactions Act, 2003 which came into operation on June 16, 2003;
- (b) the Computer Misuse Act, 2003 which came into operation on June 16, 2003; and
- (c) the Data Protection (Privacy of Personal Information) Act, 2003 which has been passed as law but is not in force yet, pending institutional appointments and arrangements.

THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT, NO. 4 OF 2003

This Act was modeled after the UNCITRAL Model Law, Bermuda, Australia and Jersey. This piece of legislation provides for the legal recognition of electronic writing, electronic contracts, electronic signatures and the original information in electronic form in relation to commercial and other transactions. Such legal recognition allows electronic communications and contracts to receive the same recognition as paper based documents. This Act also provides for electronic communications to be admissible in legal proceedings as evidence and provides that such electronic communications would not be denied admissibility solely on the basis that it is in electronic form.

Acknowledgement of receipt of electronic communications is also provided for under this Act. There are also provisions governing service providers and their responsibilities in relation to defamatory information and violation of the copyright laws.

It must be noted however that there are exclusions as to which documents will not be covered by the Act; they include:

- (a) a will or testamentary instrument or a trust;
- (b) the conveyance of real property;
- (c) a court order or official court documents;
- (d) powers of attorney as they relate to financial affairs or personal care of a person; and
- (e) other deeds and documents in section 3 of the Registration of Records Act.

THE COMPUTER MISUSE ACT, NO. 2 OF 2003

The Computer Misuse Act was modeled after the Singapore legislation. This Act criminalizes certain activities involving the unlawful use of a computer or the use of the computer with the intention to commit an offence. One of the provisions of this Act deals specifically with access to any program or data in a computer with an intent to commit an offence. The offences created include offences relating to fraud and dishonesty among others. The penalties created are summary and the fines vary from five to ten thousand dollars or imprisonment between two or three years. The Act creates a special time limit for bringing proceedings under the Act, which is twelve months from the date that evidence sufficient in the opinion of the Attorney General comes to his knowledge to warrant prosecution. However, this time limit can be no more than three years after the commission of the offence.

The Act applies to any offence so long as the accused was in The Bahamas at the material time or the computer program or data was in The Bahamas at the material time.

In this legislation the police are also given powers to seize computers, disks or other computer equipment by virtue of a warrant issued by a Magistrate under section 66 of the Criminal Procedure Code. The police are to make copies of the seized items, give such copies to the accused person and return the items to the owner within seventy-two hours.

The E-Business Office is currently in consultation with law enforcement agencies regarding the relevant legislative mechanism that would provide lawful access by such authorities to electronic transmissions consistent with the Council of Europe's Convention on Cybercrime articles dealing with appropriate changes to criminal procedure laws.

THE DATA PROTECTION (PRIVACY OF PERSONAL INFORMATION) ACT, NO. 3 OF 2003

This piece of legislation has been modeled after the Irish Act of 1988 and modified with the help of IBM Canadian lawyers, U.S. and U.K. attorneys and industry. It is also based fundamentally upon the principles established by the OECD under its Guidelines on the Protection of Privacy and Trans-border flows of Personal Data.

This Act is not yet in force since we are awaiting the appointment of a Data Protection Commissioner.

The purpose of this Act is to protect the privacy of persons in relation to personal data and to regulate the collection, processing, keeping, use and disclosure of information concerning persons in society. Obligations are placed on the Data Controller and the Data Processor. The Act applies to the public and private sectors alike. There is a Data Protection Commissioner who is responsible to ensure that all of the provisions of this Act are complied with in relation to the duties of the Data Controllers or Data Processors. The Data Protection Commissioner also is responsible for the prosecution of offences summarily under this Act. The penalties under this Act include summary conviction to a fine of two thousand dollars or on conviction on information to a fine of one hundred thousand dollars. Under this Act it is an offence for a person to obtain access to personal data without the prior authority of the data controller or data processor who keep such data and for such a person who has obtained unauthorised access to an individual's data to disclose the data to another third party.

The Act also prohibits the transborder flow of data from The Bahamas to jurisdictions that do not provide protections either by contract or otherwise equivalent to that provided under our Act.

FREEDOM OF INFORMATION ACT

The Bahamas does not have any such legislation as yet but the E-Business Development Office intends to look at a Freedom of Information Act for The Bahamas. As a precursor to this our focus is on the automation and enhancement of the Government's information systems. In relation to the information systems we want to have an effective and functioning Management Information System within the government system as well as the mechanism to facilitate this access before the Act comes into operation.

In conclusion, in The Bahamas we have a very aggressive information society agenda being led by the E-Business Development Section of the Ministry of Finance. Within this section a Legal, Regulatory and Policy Unit exists which is headed by one of the country's Information Technology lawyers.

Report on the Status of Technology Laws in Barbados

Paper Presented by the Barbados Delegation

Electronic Transactions

In 2001 Barbados enacted an Electronic Transactions Act which came into force on 8th March 2001.

The Act gives legal recognition to electronic records generally as well as to contracts formed by electronic means. In accordance with the Act, the details in relation to electronic signatures and accredited certificates are to be provided for by regulations. However, no regulations have been enacted as yet.

Electronic Evidence

There is no Electronic Evidence Act. However, the Electronic Transactions Act amended the Evidence Act to widen the definition of “document” to include information stored or recorded on tape recorder, computers or other devices and the output of such data. The Act also makes electronic records legally admissible in evidence.

Freedom of Information

Enquiries have revealed that the relevant Ministry is actively engaged in working out the policy considerations with a view to putting such legislation in place in the near future.

Privacy

There is no specific legislation which regulates personal information. The Constitution however provides a general right to privacy. If a person alleges that a Government Authority has improperly or unreasonably used any information in relation to himself, he can make a complaint to the Ombudsman under the Ombudsman Act who is authorized under that Act to make the necessary investigations.

Computer and Computer Related Crime

The relevant Ministry has made proposals for the preparation of a discussion draft Bill.

Rolanda Williams
Senior Parliamentary Counsel
21-10-2003

ANNEX 3.3

Status Report on Technology Legislation

Paper Presented by the Delegation of Belize

Belize is a very young country in full process of development. Its legislation can be no different. However, Belize has taken the bold step of attempting to bridge the gap that exists between its legislation and worldwide events. The issue of technology and cyber crime is one such area which our young country has attempted to address.

In this light, Belize has great expectations of the upcoming Workshop on Law and Technology. There is much that our country can learn from the said workshop.

➤ ***Computer and Computer Related Crimes Bill***

Currently, no legislation has been enacted in this regard. However, Belize finds the draft Bill very comprehensive and intends to use it in the near future as a guide to the enactment of similar legislation.

➤ ***Electronic Evidence Model Law***

Belize has recently enacted similar legislation in the form of the ***Electronic Evidence Act*** (No. 9 of 2003). This Act has as its objective “*to make provision for the legal recognition of electronic records and to facilitate the admission of such records into evidence in legal proceedings; and to provide for matters connected therewith or incidental thereto.*” The text of this Act is the same as that of the *Electronic Evidence Model Law*. This Act, however, has not yet entered into force.

Belize had in 1998, through an amendment to its ***Evidence Act***, Chapter 95 of the Laws of Belize, Revised Edition 2000¹, attempted to address the issue of electronic evidence. The relevant sections thereof are as follows.

83.- (1) In any civil proceedings, a statement contained in a document produced by a computer is admissible as evidence of any fact stated therein of which direct oral evidence would be admissible, if it is shown-

(a) that the document containing the statement was produced by the computer during a period over which the computer was used regularly to store and process information for the purposes of

¹ The Laws of Belize can be downloaded from www.belizelaw.org.

any activities regularly carried on over that period, whether for profit or not, by any person;

(b) that over that period there was regularly supplied to the computer in the ordinary course of those activities information of the kind contained in the statement or of the kind from which the information so contained is derived;

(c) that throughout the material part of that period the computer was operating properly or, if not, that any respect in which it was not operating properly or was out of operation during that part of that period was not such as to affect the production of the document or the accuracy of its contents; and

(d) that the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities.

(2) In any civil proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate:

(a) identifying the document containing the statement and describing the manner in which it was produced; and

(b) giving such particulars of any device involved in the production of that document as may be appropriate for the purpose of showing that the document was produced by a computer; and

(c) dealing with any of the matters to which the conditions mentioned in subsection (1) relate, and purporting to be signed by a person occupying a responsible position with relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate), shall be evidence of any matter stated therein; and for the purpose of this sub-section it is sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(3) For the purposes of this section:

(a) information is taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment; and

(b) information is taken to be supplied to a computer where, in the course of activities carried on by any individual or body,

information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities; and

(c) a document is taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

84.-(1) For the purposes of this section “business” includes every kind of business, profession, occupation, calling, operation or activity, whether carried on for profit or otherwise.

(2) In any criminal proceeding where direct oral evidence of a fact would be admissible, any statement contained in a document and tending to establish that fact shall, on production of the document, be admissible as *prima facie* evidence of that fact if -

(a) the document is, or forms part of, a record relating to any trade or business and compiled in the course of that trade or business from information supplied (whether directly or indirectly) by persons who have, or may reasonably be supposed to have, personal knowledge of the matters dealt with in the information they supply; and

(b) the person who supplied the information recorded in the statement in question is dead, or outside Belize, or unfit by reason of his bodily or mental condition to attend as a witness, or cannot with reasonable diligence be identified or found, or cannot reasonably be expected (having regard to the time which has elapsed since he supplied the information and to all the circumstances) to have any recollection of the matters dealt with in the information he supplied.

(3) For the purpose of deciding whether or not a statement is admissible as evidence by virtue of this section, the court may draw any reasonable inference from the form or content of the document in which the statement is contained, and may, in deciding whether or not a person is fit to attend as a witness, act on a certificate purporting to be a certificate of a registered medical practitioner.

85.-(1) In estimating the weight, if any, to be attached to a statement rendered admissible as evidence by virtue of this Part, regard shall be had to all the circumstances from which any inference may reasonably be drawn as to the accuracy or otherwise of the statement and in particular -

(a) in the case of a statement falling within section 83, to the question whether or not the matter which the information contained in the statement reproduces, or is derived from, was supplied to the relevant computer, or recorded for the purpose of being supplied thereto, contemporaneously with the concurrence or existence of the facts dealt with therein, and to the question whether or not any person concerned with the supply of information to that computer, or with the operation of that computer or any equipment by means of which the document containing the statement was produced by it, had any incentive to conceal or misrepresent the facts;

(b) in the case of a statement falling within any other section in this Part (other than section 83), to the question whether or not the statement was made contemporaneously with the occurrence or existence of the facts stated, and to the question whether or not the maker of the statement had any incentive to conceal or misrepresent the facts.

(2) For the purpose of any rule of law or practice requiring evidence to be corroborated or regulating the manner in which uncorroborated evidence is to be treated, a statement rendered admissible as evidence by this Part shall not be treated as corroboration of evidence given by the maker of the statement.

86.-(1) Subject to subsection (2), in any proceedings whether civil or criminal, an instrument to the validity of which attestation is requisite may, instead of being proved by an attesting witness, be proved in the manner in which it might be proved if no attesting witness were alive.

(2) Subsection (1) shall not apply to the proof of wills or other testamentary documents.

87. In any proceedings, whether civil or criminal, there shall, in the case of a document proved, or purporting, to be not less than twenty years old, be made any presumption which immediately before the commencement of this Act would have been made in the case of a document of like character proved, or purporting, to be not less than thirty years old.

88. Section 95 of the Supreme Court of Judicature Act (which relates to the making of rules of court) authorises the making of rules of court providing for orders being made at any stage of any proceedings directing that specified facts may be proved at the trial by affidavit with or without the attendance of the deponent for cross-

examination, notwithstanding that a party desires his attendance for cross-examination and that he can be produced for that purpose.

➤ ***Electronic Transactions Model Law***

Belize has enacted the ***Electronic Transactions Act*** (No. 8 of 2003). The text thereof has been adapted from the Electronic Transactions Model Law and is identical to it. However, this Act has not yet entered into force.

➤ ***Freedom of Information Act***

Since 1994 Belize enacted its ***Freedom of Information Act*** (hereinafter, “the Belize Act”), Chapter 13 of the Laws of Belize, Revised Edition 2000. The text of this Act coincides with most of the text contained in Draft Act (that is, the Draft sent to the countries for their consideration), with very few exceptions. For example, the Draft exempts the Prime Minister and any Commission of Enquiry appointed by him whereas the Belize Act does not contain such provisions.

Additionally, whereas the Draft Act provides for Judicial Review under s. 41, the Belize Act contains a separate Part (Part V) entitled “Review of Decisions”. Under the provision of this Part, applications can be made to the Ombudsman² for the review of a decision refusing to grant access to a document pursuant to a request. The relevant sections are as follows.

PART V

Review of Decisions

35.-(1) Application may be made to the Ombudsman for review of a decision refusing to grant access to a document in accordance with a request or deferring the provision of access to a document.

(2) Subject to subsection (3), in proceedings under this Part, the Ombudsman has power, in addition to any other power, to review any decision that has been made by a Ministry or prescribed authority in respect of the request and to decide any matter in relation to the request that, under this Act, could have been or could be decided by a Ministry or prescribed authority, and any decision of the Ombudsman under this section has the same effect as a decision of the Ministry or prescribed authority.

(3) Where, in proceedings under this section, it is established that a document is an exempt document, the Ombudsman does not have

² The Ombudsman (or Parliamentary Commissioner) is appointed under the Ombudsman Act, Chapter 5 of the Laws of Belize, Revised Edition 2000. He is appointed by the Governor General acting on the recommendation of both Houses of the National Assembly contained in resolutions passed by them. He hold office for a period of three (3) years but is eligible for reappointment at the expiration of the period.

power to decide that access to the document, so far as it contains exempt matter, is to be granted.

(4) Where, under a provision of Part IV, it is provided that a certificate of a specified kind establishes conclusively, for the purposes of this Act, that a document is an exempt document and such a certificate has been given in respect of a document, the powers of the Ombudsman do not extend to reviewing the decision to give the certificate or the existence of proper grounds for the giving of the certificate.

(5) The powers of the Ombudsman under this section extend to matters relating to fees and charges payable under this Act in relation to a request.

36.-(1) Where a decision has been made, in relation to a request to a Ministry or prescribed authority, otherwise than by the responsible Minister or principal officer (not being a decision on a review under this section), the applicant may, within 28 days after the day on which notice of the decision was given to the applicant in accordance with section 21, apply to the responsible Minister or principal officer concerned for a review of the decision in accordance with this section.

(2) A person is not entitled to apply to the Ombudsman for a review of a decision in relation to which subsection (1) applies unless-

(a) he has made an application under that subsection in relation to the decision; and

(b) he has been informed of the result of the review or a period of 14 days has elapsed since the day on which he made that application.

(3) Where an application for a review of a decision is made to the responsible Minister or the principal officer in accordance with subsection (1), he shall forthwith arrange for himself or a person (not being the person who made the decision) authorized by him to conduct such reviews to review the decision and to make a fresh decision on the original application.

37.-(1) Where -

(a) an application for review of a decision has been made in accordance with section 36; and

(b) the application for review is refused or the applicant has not been informed of the result of the review within 14 days after the day on which he made that application, the applicant may apply to the Ombudsman for review of the decision refusing to grant access to a document, within 21 days of the date on which he is notified of the decision refusing the review or within 21 days after the expiry of the period of 14 days mentioned in paragraph (b) of subsection (1) above.

(2) Where –

(a) a request has been made to a Ministry or prescribed authority in accordance with section 16; and

(b) a period of 14 days has elapsed since the day on which the request was received by or on behalf of the Ministry or prescribed authority; and

(c) notice of a decision on the request has not been received by the applicant, the principal officer shall, for the purpose of enabling an application to be made to the Ombudsman under section 35, be deemed to have made on the last day of that period, a decision refusing to grant access to the document, and the applicant may apply to the Ombudsman to grant access to the document in question within 21 days of the expiry of the said period of 14 days.

(3) Before dealing further with an application made by virtue of this section, the Ombudsman may, on the application of the Ministry or prescribed authority concerned, allow further time to the Ministry or prescribed authority to deal with the request.

(4) Notwithstanding the period of limitation mentioned in this section, the Ombudsman may, in his discretion, grant further time to the applicant if he is of the opinion that there has been no unreasonable delay in making the application.

38. In proceedings under this Part, the Ministry or prescribed authority to which or to whom the request was made has the onus of establishing that a decision given in respect of the request was justified or that the Ombudsman should give a decision adverse to the applicant.

39. In proceedings under this Part, the Ombudsman shall make such order as he thinks necessary having regard to the nature of the proceedings and, in particular, to the necessity of avoiding the disclosure to the applicant of exempt matter.

40.-(1) Where there are proceedings before the Ombudsman under this Act in relation to a document that is claimed to be an exempt document, and the Ombudsman is not satisfied, by evidence on affidavit or otherwise that the document is an exempt document, he may require the document to be produced for inspection by him only and if, upon the inspection, he is satisfied that the document is an exempt document, he shall return the document to the person by whom it was produced without permitting any other person to have access to the document or disclosing the contents of the document to any other person.

(2) The Ombudsman may require the production, for inspection by him only, of an exempt document for the purposes of determining whether it is practicable for a Ministry or prescribed authority to grant access to a copy of the document with such deletions as to make the copy not an exempt document and, where an exempt document is produced by reason of such a requirement, he shall return the document to the person by whom it was produced without permitting any other person to have access to the document, or disclosing the contents of the document to any other person.

(3) Notwithstanding subsections (1) and (2) but subject to subsection (4), the Ombudsman is not empowered in any proceedings to require the production of a document in respect of which there is in force a certificate under section 22 or 23.

(4) Where a certificate of a kind referred to in sub-section (3) identifies a part or parts of the document concerned in the manner provided in section 22 (3) or 23 (3), subsection (3) of this section does not prevent the Ombudsman from requiring the production, in proceedings before him under this Act in relation to the document, of a copy of so much of the document as is not included in the part or parts so identified.

41. In proceedings before the Ombudsman under this Part, evidence of a certificate under section 22 or 23, including evidence of the identity or nature of the document to which the certificate relates, may be given by affidavit or otherwise and such evidence is admissible without production of the certificate or of the document to which it relates.

42. For the purposes of performing his functions under this Act, the Ombudsman shall have the same powers as a Magistrate in respect of the attendance and examination of witnesses.

43. Any party dissatisfied with a decision of the Ombudsman under this Act may appeal to the Supreme Court, and in every such case the provisions of Part X of the Supreme Court of Judicature Act and the rules made thereunder shall *mutatis mutandis* apply.

➤ **Privacy Act**

No similar enactment has been passed in Belize. However, protection of the privacy of all persons in Belize is guaranteed by the Belize Constitution Act (hereinafter “the Constitution”), Chapter 4 of the Laws of Belize, Revised Edition 2000. Section 3 thereof provides that “*every person in Belize is entitled to the fundamental rights and freedoms of the individual . . . whatever his race, place of origin, political opinions, color, creed or sex, but subject to the respect for the rights and freedoms of others and for the public interest.*” These rights include the right for “protection of his family life, his personal privacy, the privacy of his home and other property and recognition of his human dignity.”

Section 14 of the Constitution provides that “a person shall not be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. The private and family life, the home and the personal correspondence of every person shall be respected.”

October 29th 2003

Iran Tillett-Dominguez (Mrs.)
Crown Counsel
Attorney General’s Ministry
East Block
Belmopan, BELIZE, Central America

E-Mail: iran_tillett@yahoo.com

ANNEX 3.4

Paper Presented by the Dominica Delegation

We do not appear to have legislation respecting technology except for a few provisions in the Evidence Ordinance Cap. 64, the Laws of Dominica, providing for the admissibility of statements contained in documents produced by computers. The admissibility of such statements relates to both civil and criminal proceedings. The relevant Act is the Evidence (Amendment) Act 2001, Act No. 1 of 2001.

Nevertheless, the Government of the Commonwealth of Dominica (the Government) has given the emerging electronic environment a prominent position on its agenda. This positioning is informed by several factors respecting the application of information and communications technologies. First, the Government is mindful that information and communications technologies (ICT) can be a catalyst to economic and social development.

Secondly, ICT are considered as appropriate vehicles for improving the delivery of government programmes and services to its relevant constituents. A corollary to the second factor is the expected improvement in efficiency and effectiveness of the public service and the resulting realization of an improved quality of life for the peoples of Dominica coupled with the improved competitiveness of the country.

Thirdly, the Government recognizes that an integrated policy respecting ICT would encompass effective strategies, tools and techniques to help the general populace of Dominica. And fourthly, the Government is committed to transacting business in a trustworthy environment based on records that are authentic, reliable, accessible, understandable and usable.

Unfortunately there is no single or specific document outlining the policy of the Government respecting ICT. However, such a policy may be gleaned from several sources and actions. In this regard I need only to mention three of sources and actions:

- One, in 2000, the Government and those of four other OECS countries signed a Treaty Establishing the Eastern Caribbean Telecommunications Authority. The Telecommunications Act 2000, Laws of Dominica provides for the implementation of the Treaty in Dominica. The principal object and purpose of that Act is to provide for the liberalization of the telecommunication sector.
- Two, in July of 2001 the Government in advancing a policy to make ICT widely available, accessible and affordable reduced the import duty on

computer software from 35 % to 5 % and removed the Consumption Tax on computer and computer software.

- Three, the Government has encouraged and continues to encourage the development of individual ministerial ICT policy with the intention of collapsing these individual ICT policies into a comprehensive national ICT policy.

The various ministerial ICT policies can properly be considered as being in the infant stage of development. The issues that those ministries seek to address include the following:

1. What information needs to be created and acquired and for what purposes?
2. Who will have access to the information created or acquired?
3. Whether information created or acquired will be shared, combined and integrated to solve increasingly interconnected problems?
4. Whether the information created or acquired will be used to promote political and public debate and genuine stakeholder participation?
5. Who will use and control the information?
6. How will the security, integrity and value of the information created or acquired be protected?
7. Who will ultimately be responsible for making decisions respecting issues 1 to 6?

The development of these policies has proven to be more challenging in the absence of the necessary information respecting international and other national legal frameworks for e-commerce and e-government. In addition, there is uncertainty whether our present laws are adequate to address issues or disputes which may arise in respect to electronic transactions that occur within the State a fortiori cross-border electronic transactions between buyers and sellers.

Other un-charted areas regarding electronic activities and transactions including jurisdiction of national courts, legal effect of certain actions, and the concept of electronic signature pose their own unique challenges. Moreover, the issues of identity theft, forgery and other related electronic / cyber crimes present different challenges.

Globalization has resulted in the creation of what may be described as an information and technology-rich environment. And the Government is of the view that its ICT policy ought to reflect certain principles and values namely –

- Respect for the rule of law;
- Citizens participation and access to information;
- Ethical conduct;
- Privacy and security;
- Transparency and openness; and
- Accountability.

In short, there are many unidentified risks associated with the implementation of a policy respecting ICT. The basic issue that needs addressing is whether the State is able to utilize ICT to improve on the delivery of programmes and services without compromising the constitutional principle of good governance.

It follows from the foregoing that Dominica cannot speak of having in place a robust and adequate information infrastructure that is able to ensure the integrity of government-held information, *a fortiori*, support the deeper dimensions of e-government, e-commerce or the adoption of e-government strategies.

We wish to express our profound gratitude to the Commonwealth Secretariat for convening this Workshop on Law and Technology and we look forward to meaningful participation. It is our hope that our participation at this Workshop will assist us in putting in place a robust and adequate information infrastructure that would be able -

- (a) to ensure the integrity of government held information;
- (b) to support the deeper dimensions of e-government and e-commerce;
- (c) to support the adoption of e-government strategies.

Mr John Elue Charles
Chief Parliamentary Draftsman
Ministry of Legal Affairs
Commonwealth of Dominica

COMMONWEALTH REGIONAL WORKSHOP ON LAW AND TECHNOLOGY

Paper Presented by the Delegation of Guyana

In recognition of the technological advancement in recent years, and of the inadequacy of our Evidence Act, Chapter 5:03 to deal with these advances, Guyana has, in October of 2002, amended its legislation with respect to Electronic Evidence. The Evidence (Amendment) Act, 2002 No. 10 of 2002, an Act to amend the Evidence Act, makes significant inroads to the issue of admissibility of electronic evidence.

For instance, the Evidence (Amendment) Act makes provisions for the admissibility of statements contained in documents produced by computers as evidence of any fact stated therein. By virtue of Section 91(1), the conditions to be satisfied before such evidence is admitted include, *inter alia*, “that the document containing the statement was produced by the computer during a period over which the computer was used regularly to store and process information for the purposes of any activities regularly carried in over that period...” and “that throughout the material part of that period the computer was operating properly or, if not, that any respect in which it was not operating properly or was out of operation during that part of that period was *not such as to affect the production of the document or the accuracy of its contents...*”

Further, by Section 91(2), where it is desired to give a statement in evidence under the aforementioned provisions, a certificate (a) identifying the document containing the statement and describing the manner in which it was produced; and (b) giving such particulars of any device involved in the production of that document as may be appropriate for the purpose of showing that the document was produced by a computer; and (c) dealing with any of the matters to which the conditions mentioned in subsection (1) relate, and purporting to be signed by a person occupying a responsible position with relation to the operation of the relevant device or the management of the relevant activities...” shall be evidence of any matter stated therein; and for the purpose of this subsection *it is sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.*”

It should however be noted that the provisions outlined above are applicable only to civil proceedings. The Act also deals with the weight to be attached to evidence, and also deals with “electronic signatures” in any legal proceedings, and matters connected thereto.

With respect to Electronic Transactions although there is no enacted legislation as yet, consideration is now being given to a Draft E-Commerce Bill. However, at this stage the

Bill is still a working document and is undergoing changes. The Draft E-Commerce Bill draws from Acts and Bills from other Jurisdictions which are partly based on the UNCITRAL Model Law. One objective of the Bill is to establish and clarify the legal basis of e-commerce.

Like the Commonwealth Secretariat Electronic Transactions Bill, our Draft E-Commerce Bill has a section dealing with the legal recognition of electronic communications – “an electronic communication shall not be denied legal effect, validity, admissibility or enforceability solely on the ground that it is in electronic form”. Also, a section stating that the requirement that information must be in writing is met if that information is contained in an electronic communication, provided that that information is accessible to and is capable of retention by the intended recipient.

There are also provisions dealing with the retention/keeping of documents, records or information and the conditions that apply thereto; the recognition of foreign electronic signatures/documents; contracts; the exclusion of the operation of the proposed Bill, among other provisions.

As regards the other Model Bills to be discussed at the Workshop – Freedom of Information, Privacy and Computer and Computer Related Crime - Guyana does not have any enacted legislation, and would consider the Model Laws provided by the Commonwealth Secretariat with a view to future enactment. Guyana looks forward to participating in the upcoming workshop, and learning from other jurisdictions which already have these Laws in place.

Guyana also takes the opportunity to laud the efforts of the Commonwealth Secretariat in organizing this Workshop, which comes at an opportune time.

Damone Younge
STATE COUNSEL
Attorney General’s Chambers and
Ministry of Legal Affairs,
95 Carmichael Street,
Georgetown, Guyana.

Nareshwar Harnanan
STATE COUNSEL
Attorney General’s Chambers and
Ministry of Legal Affairs,
95 Carmichael Street,
Georgetown, Guyana.

ANNEX 3.6

COMMONWEALTH REGIONAL WORKSHOP ON LAW AND TECHNOLOGY
Paper Presented by the Delegation of Jamaica

1. The revolution of Information and Communication Technologies (ICTs) presents numerous opportunities and challenges to countries in the developing world. The Government of Jamaica has recognized that a lack of infrastructure, both legal and otherwise, shortage of relevant skills and inadequate investment in technological development can affect progress towards exploiting the new generation of ICTs.
2. In this regard, the ICT sector has been identified as a critical component in the generation of economic growth. In recognition of the benefits emerging from this sector, the main focus has been on (i) the liberalization of the telecommunications industry - which has seen the introduction of a new Telecommunications Act and (ii) the promotion of Electronic Commerce.
3. An environment that is conducive to conducting business and sharing information with confidence is essential to the promotion of electronic commerce. The Government's role in this process has been to provide support by setting policy and regulatory framework that is relevant to the ICT sector, while taking cognisance of the pervasive nature of electronic commerce and the challenges pertaining to legal and security matters.
4. An analysis of the current legislative framework in Jamaica demonstrates that focus is placed mainly on paper-based, commercial transactions. The statutes that provide the regulation for commercial banking, trade and other financial relationships contain elements of the pre-computer era and as such cannot effectively respond to electronic commerce issues. An appropriate legal framework that addresses those issues will therefore be necessary.
5. We are at an advanced stage in this process, to the point where a draft **Electronic Transactions Bill** is currently the subject of commentary.
6. The Bill primarily takes into account the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce (1996) and the Commonwealth Secretariat Model Law on Electronic Commerce and Computer Crime. It also draws from other legislative models including those of Australia, Bahamas, Bermuda and Canada in an effort to comprehensively address all the relevant issues.
7. The broad issues covered in the Bill relate to the (i) recognition of electronic forms of writing, (ii) formation and validity of electronic agreements and transactions, (iii) the recognition and authentication of electronic signatures, (iv) attribution of electronic communication (iv) admissibility of electronic forms of evidence.

8. On the issue of electronic evidence, our Evidence Act was amended to permit the admissibility of computer generated documentary evidence provided that those documents satisfied specific authentication criteria. The proposed Electronic Transactions Act will now extend the category of electronic evidence that is admissible, to specifically include information contained in computer programs, software and databases. Particular mention should also be made of our Supreme Court of Jamaica Civil Procedure Rules 2002 which gives the court a discretionary power to permit witness testimony through a video link. The reform of our laws in this regard is an innovative step in the thrust towards taking advantage of the opportunities presented in an electronic environment.
9. The movement towards enacting appropriate e-commerce legislation has impressed upon the Government of Jamaica the urgency in addressing those inescapable, computer related crime issues. If these issues remain unchecked, they may serve as an impediment in the advancement of an e-commerce environment and consequently inhibit the general use of information and computer technology.
10. Computer related crime is a new legal phenomenon in Jamaica. Different varieties of computer crime can be devised, and it is important to understand how they differ from real world criminal activity, why it is a matter of global concern and its incidence and costs. It is worthy to note that in recent times there have been reports of computer systems within Jamaica, both individual and corporation, being exposed to destructive computer viruses and hacker intrusions which originated from other jurisdictions. It is the trans-national nature of these crimes that necessitates uniform laws and international cooperation.
11. The focus of our criminal law legislation is on the traditional crimes such as theft, fraud and criminal damage to property. The use of technology in the commission of these crimes may not have been contemplated at the time the provisions were formulated. It might however be possible to apply an interpretation to the relevant provisions, in order to bring within the coverage of existing legislation, those criminal acts that are computer aided. For example, if we examine the activity of damaging computer data – this can be dealt with under our Malicious Injuries to Property Act. Under that Act, it is an offence to damage public or private property. The Act however does not stipulate the method through which that property must be damaged in order to constitute the offence. One can therefore argue that damage to computer data by a virus may fall within the scope of the Act.

12. Similarly, in dealing with the act of computer related fraud, the Larceny Act makes it an offence for a person, by false pretence, to defraud another person. Again, this Act does not specify the method through which the fraudulent activity should have been committed. The presumption therefore is that the commission of the fraudulent activity, by use of a computer, will fulfil an element of the offence.
- 13.
14. Notwithstanding the existence of these and similar provisions, the Government is of the view that there is need for appropriate legislative provisions which comprehensively addresses the computer crime issues in a holistic manner. Leaving provisions to judicial interpretation may result in legislative uncertainty and consequently may not be the best approach to adopt.
- 15.
16. Critical to the process therefore, is the development of a legal regime in order to introduce criminal legislation that will effectively deal with the security concerns that may arise from the use of computer technology. In this exercise, we intend to extend the criminal law by introducing new offences which will provide the necessary protection for persons operating within the electronic environment.
17. The proposed legislation will take into account the Commonwealth Model Law on Computer Crime and the Council of Europe Draft Convention on Cyber-crime and we will also draw from other legislative models including the United States, United Kingdom, South Africa, Singapore and Canada in confronting the issues.
18. The issues currently under consideration include:
 - (i) law that covers both criminalisation provisions and other connected provisions in the area of computer or computer-related crime. These provisions will define the different categories of offences and then deal with liability and sanctions. It will be necessary to examine offences such as illegal access, illegal interception, data interference, system interference, computer-related forgery and fraud, offences related to child pornography and copyright,
 - (ii) preservation of stored data; disclosure of data; production order; search and seizure of computer data; real-time collection of data; interception of content data,
 - (iii) development and trafficking in devices or applications primarily used to obtain unauthorised access,
 - (iv) trafficking in computer passwords,

- (v) review of all existing search and seizure powers, whether statutory or by common law and ensuring that all such powers extend to search and seizure in the computer context,
- (vi) unauthorised damage of data stored by way of virus infections,
- (vii) the admissibility and disclosure of electronic evidence and the question of whether the rules that apply to other forms of documentary evidence can similarly apply to electronic documents,
- (viii) the potential for the misuse of computer technology through terrorist attacks on information systems or the terrorist use of such technology to facilitate the commission and financing of the prohibited act,
- (ix) the extradition laws as they relate to the procedures to be applied when bringing an offender before a national court,
- (x) the scope of the mutual criminal assistance provisions in regards to facilitating requests relating to computer data, preservation orders, disclosure and collection of data, access to computer data and seizure with the appropriate judicial safe guards,
- (xi) cyber-crime and its relation to money laundering activities,
- (xii) balancing international and national security interests against those of good governance and the erosion of fundamental liberties.

The expectation is that on passage through Parliament, of both the Electronic Transactions Act and the Cyber-crime legislation, Jamaica would be in a commanding position to respond to the challenges presented by the innovations of computer technology in this interconnected, competitive, global environment.

Mrs. Marlene Lynch Aldred
 Attorney General's Chambers
 2nd Floor, NCB North Tower
 2 Oxford Road
 Kingston 5
 Jamaica.
 E-mail: marlene.aldred@agc.gov.jm

Mr. José Griffith
 Legal Reform Department
 1st Floor, NCB North Tower
 2 Oxford Road
 Kingston 5
 Jamaica.

E-mail: jsg2000@hotmail.com

ANNEX 3.7

COMMONWEALTH REGIONAL WORKSHOP ON LAW AND TECHNOLOGY

Paper Presented by the St Lucia Delegation

REPORT ON THE STATUS OF TECHNOLOGY LEGISLATION IN ST LUCIA

Currently Saint Lucia is in the process of developing a comprehensive set of legislation in relation to cyber crime and related matters. Hence, Saint Lucia will be represented at the Commonwealth Regional Workshop on law and technology and will to some degree adopt/adapt the model laws as appropriate.

There is legislation already in existence in Saint Lucia which touch and concern cyber crime and related matters. For example:

- The Evidence Act No. 5 of 2002 (Not yet in force)
- The Protection of Privacy Act (Still a draft Bill)
- The Freedom of Information Act (Still a draft Bill)
- The Draft Criminal Code (Still a draft Bill)

The Evidence Act No. 5 of 2002 is an Act to reform the law relating to evidence in proceedings in courts in Saint Lucia and to provide for related matters. In the Evidence Act No. 5 of 2002 electronic evidence is recognized. In section 2 “copy” includes any readable reproduction of document, microfiche *et cetera*. “Device” includes computer. “Document” means anything on which information of any description is recorded.

The Protection of Privacy Act is an Act to make provision for the promotion and protection of the privacy of individuals, and for connected matters. It is based on the commonwealth draft model legislation. In this Act “document” means any medium in which information is recorded, whether printed or on tape or on tape or film or by electronic means or otherwise and includes ...machine-readable record or any record which is capable of being produced from a machine-readable record by means of equipment or a programme (or a combination of both) which is used for that purpose by the public authority which holds the record. Note whilst Part III of the model Privacy Act provides for the creation of the office of the Privacy Commissioner to carry out the investigations under Part IV, we in Saint Lucia conferred these powers on the Parliamentary Commissioner an office already in existence under the Saint Lucia

Constitution Order 1978 and as such guaranteed the same authority as envisaged in Part III of the draft model.

The Freedom of Information Act is an Act to provide to Saint Lucia citizens and persons residing permanently in Saint Lucia, a general right to access to official records and for connected matters. It is based on the commonwealth draft model legislation. In this Act “document” includes ... any disc ...or other device in which sounds or other device data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom [or] ...any film... or other device in which one or more visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom.

The Draft Criminal Code in section 267 deals with computer fraud.

“Computer fraud

267. (1) A person who, with intent to defraud or deceive-

- (a) alters, damages. Destroys or otherwise manipulates data or programmes held in or used in connection with a computer or computer network by adding to, erasing or otherwise altering the data or programme; or
- (b) does any act which causes an unauthorized modification of the contents of a computer network; is guilty of an offence and liable on conviction on indictment to imprisonment for fifteen years.

(2) a modification of the contents of a computer is unauthorized-

- (a) if the person who causes it is not himself or herself entitled to determine whether the modification should be made; and
- (b) if the person does not have the consent of the person who is entitled to grant consent for the modification.

(3) In this section-

“computer” means any devise for storing and processing information;

“computer network” means the interconnection of two or more coputers, whether geographically separated or in close proximity, or the interconnection of communication systems with a computer through terminals whether remote or local;

“modification of the contents of a computer” includes the alteration of the programme or data held in a computer or any addition to the contents of a computer of a programme or data.”

The draft Bills provided, that is:

- The Computer and Computer Related Crimes Bill
- The privacy Act [...]
- Freedom of Information Act [...]
- The Electronic Evidence Model Law

were all reviewed and as stated before a draft Protection of Privacy Bill and Freedom of information Bill are already in existence in Saint Lucia. The need for legislation that speaks directly to cyber crime and related matters is obvious.

The draft legislation in Saint Lucia was informed by the draft bills provided and the following legislation from the Bahamas and Singapore:

- The Computer Misuse Bill, 2003 (Bahamas);
- The Electronic Communications and Transactions Act, 2003 (Bahamas) ;
- The Data Protection (Privacy of Personal Information) Act, 2003 (Bahamas);
- The Electronic Transactions Act 1998 (Singapore).

Close attention will be paid to the reports of the delegates from other jurisdictions with respect to The Computer and Computer Related Crimes Bill and The Electronic Evidence Model Law. We look forward to a successful workshop.

Ms Fikile Dlamini

The Director of Legislative Drafting Department of the Attorney General's Chambers

Ms Allison Isaac

Legislative Drafter 1

ANNEX 3.8

REPORT ON THE STATUS OF TECHNOLOGY LEGISLATION IN ST VINCENT AND THE GRENADINES

Paper Presented by the Delegation of St Vincent and the Grenadines

1. Both the Freedom of Information Act and the Privacy Act were passed in the House of Assembly on the 27th June, 2003.

The object of the Freedom of Information Act is to safeguard the right of members of the public to access information held by public authorities with the aim of increasing transparency and accountability of government. The object of the Privacy Act is to promote and protect the privacy of individuals. It is also aimed at collecting, holding, using, correcting and disposing of personal information in a manner that recognises the right to privacy of individuals with respect to their personal information. The Privacy Act has already been assented to. The Freedom of Information Act has not.

2. There are no other pieces of legislation which deal with technology per se save and except section 50 of the Evidence Act Cap. 158 of the Laws of Saint Vincent and the Grenadines which provides for the admissibility of statements contained in a document produced by a computer as evidence in civil proceedings.
3. In 2001 the Ministry of Telecommunications, Science, Technology and Industry was established for the first time in Saint Vincent and the Grenadines. This was in response to the Government's awareness that technology has become an integral feature of modern day society and plays a critical role in the functioning of government and in the running of today's modern societies. This new ministry is in need of a legislative framework that would enable a more efficient and effective functioning of the Ministry. This is a technical area and the Attorney General's Chambers, more particularly the drafting department has no expertise and little to no skill and knowledge where technology legislation is concerned. Indeed this workshop will play a role in equipping us to deal with technology legislation.

**Ministry of Legal Affairs
Attorney General's Chambers
St Vincent and the Grenadines**

ANNEX 4 – LIST OF PARTICIPANTS

ANNEX 4

List of Participants

COUNTRY	DETAILS
THE BAHAMAS	<p>Ms Sherece Verdette Gibson Senior Counsel Office of the Attorney General Third Floor, Post Office Building East Hill Street, Nassau Bahamas PO Box N-3007 Tel: 001 242 5020446 001 242 5020400 Fax: 001 242 3222 2255 Email: gibsonsv@hotmail.com</p>
BARBADOS	<p>Mrs Rolanda Williams Senior Parliamentary Counsel Attorney General's Chambers 3rd Floor, Frank Walcott Building Culloden Road St. Michael, Barbados Tel: 001 246 431 7749/05 Fax: 001 246 435 9533 Email: rwilliams@cpbarbados.gov.bb</p>
BELIZE DOMINICA	<p>Mrs Iran Tillett-Dominguez Crown Counsel Attorney General's Ministry East Block Belmopan City Belize, Central America Tel: 00 501 822 2504 Fax: 00501 822 3390 Email: iran_tillett@yahoo.com</p> <p>Mr John Elue Charles Chief Parliamentary Draftsman Ministry of Legal Affairs Immigration and Labour Attorney General's Chambers Government Headquarters Roseau Commonwealth of Dominica Tel: 001 767 448 2401 (ext 3294/3298) Fax: 001 767 448 0182 Email: legallaffairs@cwdom.dm</p>

DOMINICA (continued)	Miss Pearl Richards State Attorney Ministry of Legal Affairs Immigration and Labour Attorney General's Chambers Government Headquarters, Kennedy Avenue Roseau Commonwealth of Dominica Tel: 001 767 448 2401 (ext 3294/3298) Fax: 001 767 448 0182 Email: legalaffairs@cwdom.dm
GRENADA	Danine Kami Jones Crown Counsel I Attorney General's Chambers Ministry of Legal Affairs, Methodist Building, Kingston St Vincent and the Grenadines Tel: (473) 440 2050 Fax: (473) 440 3121 E mail: danine@yahoo.com legalaffairs@caribsurf.com/ranthony@caribsurf.com
GUYANA	Miss Damone Younge State Counsel Attorney General's Chambers & Ministry of Legal Affairs 95 Charmichael Street Georgetown, Guyana Tel: 001 592 225 3607/592 226 2616 – 8 Fax: 001 592 227 5419 E mail: damonefjyounge@yahoo.com Mr. Nareshwar Harnanan State Counsel Attorney General's Chambers & Ministry of Legal Affairs 95 Charmichael Street Georgetown, Guyana Tel: 001 592 225 3607(Work)/592 226 2616 – 8 001 592-226-0604 (Home) Mobile: 001 592 623 0308 Fax: 001 592 227 54 19 E mail:nareshwarharnanan@justice.com

JAMAICA	<p>Mrs Marlene Aldred Divisional Director (Ag.) Attorney General's Chambers 2nd Floor – NCB North Tower Mutual Life Building 2 Oxford Road Kingston 5 Tel: (876) 906-7120. Fax: (876) 906 7665 Email: marlene.aldred@mnsj.gov.jm Marlene.aldred@agc.gov.jm</p> <p>Mr Jose Griffiths Senior Legal Officer Legal Reform Department 1st Floor, NCB North Towers Mutual Life Building 2 Oxford Road Kingston 5 Jamaica Tel: (876) 906 4908-24 or 906 4139 Fax: (876) 906 0287 Email: rd@mail.infochan.com or jsg2000@hotmail.com or jose.griffith@mnsj.gov.jm</p> <p>Miss Judith Grant Parliamentary Counsel Office of the Parliamentary Counsel 1st Floor North Tower NCB Towers 2 Oxford Road Kingston 5 Email: Jag@jamaicans.com</p>
ST KITTS AND NEVIS	<p>Miss Karen Hughes Parliamentary Counsel Ministry of Justice and Legal Affairs Government Headquarters P O Box 164 Church Street Basseterre St Kitts and Nevis Tel: 00 1 869 465 2521</p>

<p>ST KITTS A ND NEVIS (continued)</p>	<p>Fax: 00 1 869 465 5040 Email: attnygenskn@caribsurf.com blestkay@yahoo.com</p> <p>Mr Stephen Hector Attorney General's Chambers Government Headquarters P O Box 164 Church Street Basseterre St Kitts and Nevis Tel: 00 1 869 465 2521 Fax: 00 1 869 465 5040 Email: attnygenskn@caribsurf.com</p>
<p>ST LUCIA</p>	<p>Ms. V. Fikile Dlamini Director of Legislative Drafting Attorney General's Chambers 2nd Floor, NIS Building Waterfront, Castries St Lucia Tel: 001 (758) 468 3248/451 9836 Fax: 001 (758) 458 1131 Email: vfdlamini@hotmail.com legislativedrafting@yahoo.com</p> <p>Miss Allison Isaac Legislative Drafter1 The Legislative Drafting Department Attorney General's Chambers Old Ministry of Education Building Corner of Micoud & Laborie Street Castries St Lucia Tel: (758) 468 3200 Fax: (758) 458 1131 Email: allisaac@hotmail.com drafting2003@hotmail.com legislativedrafting@yahoo.com</p>
<p>ST VINCENT AND THE GRENADINES</p>	<p>Ms Danine Jones Crown Counsel I Ministry of Legal Affairs</p>

	<p>Attorney General's Chambers Granby Street, Kingstown St Vincent & the Grenadines Tel: 00 1 784 457 2807 or 1 784 456 1762 Fax: 00 1 784 457 2898 Email: att.gen.chambers@vincysurf.com</p>
TRINIDAD & TOBAGO	<p>Mr. Samraj Harripaul Senior Parliamentary Counsel Law Reform Commission Trinidad & Tobago Tel: 001 868 623 1819/624 2077 Ext 2522 (Work) 001 868 665 6108 (Home) 624 0746 Email: law reform @ ag.gov.tt</p> <p>Ms. Lorraine John Acting Parliamentary Counsel II Legislative Drafting Department Ministry of the Attorney General Trinidad and Tobago Tel: 001 868 623 5886 Ext 2422 (Work) 001 868 624 8681 001 868 675 2188 (Home) 001 868 689 9976 (Cell) Fax: 001 868 625 8121 Email: Injohn26@hotmail.com permsec@ag.gov.tt</p>
CARICOM	<p>Mr Duke Pollard Director CARICOM Legislative Drafting Facility CARICOM Secretariat Juman Building, 57 High Street PO Box 10827 Georgetown Guyana Tel: 1 (592) 227 8867 Fax: 1 (592) 226 7816 Email: legal2@caricom.org</p> <p>Ms Alexis Downes-Amsterdam Draftsperson CARICOM Legislative Drafting Facility</p>

	<p>CARICOM Secretariat Juman Building, 57 High Street Kingston, PO Box 10827 Georgetown Guyana Tel: 1 (592) 223 6455 - 6 Fax: 1 (592) 223 6453 Email: cldf@caricom.org alexis@caricom.org</p>
<p>RESOURCE PERSONS</p>	<p>Jeff Cumberbatch Deputy Dean, Faculty of Law University of West Indies Cave Hill Campus PO Box 64 Bridgetown, Barbados Tel: 001 246 417 4217/4223 Fax: 001 246 424 1788 Email: jcumberbatch@uwichill.edu.bb or jeflaw75@yahoo.com</p> <p>Ms Lucie Angers Department of Justice Room 5021 East Memorial Building 284 Wellington Street Ottawa, Ontario K1A 0H8</p> <p>Canada Tel: 00 1 613 957 4750 Fax: 00 1 613 957 6374 Email: langers@justice.gc.ca</p>
<p>COMMONWEALTH SECRETARIAT</p>	<p>Ms Cheryl Thompson-Barrow Deputy Director, Head, Law Development Section Legal and Constitutional Affairs Division</p> <p>Mr Rogers W'O Okot Uma Chief Programme Officer Head , Infomatics</p>

	<p>Governance and Institutional Development Division</p> <p>Dr Emmanuel Opoku Awuku Senior Programme Officer Justice Section Legal and Constitutional Affairs Division</p> <p>Mrs Aruna Narain Chief Programme Officer Criminal Law Section Legal and Constitutional Affairs Division</p> <p>Ms Margaret Bruce Programme Officer Law Development Section Legal and Constitutional Affairs Division</p> <p>Mrs Amina Hussein Executive Officer Governance and Institutional Development Division</p>
--	---

ANNEX 5 – AGENDA



Law and Technology Workshop for the Caribbean

Terra Nova Hotel, Kingston, Jamaica

November 3 – 7, 2003

Presented by

**The Legal and Constitutional Affairs Division (LCAD) of
the Commonwealth Secretariat**

In collaboration with

**The Governance and Institutional Development Division (GIDD)
of the Commonwealth Secretariat**

A G E N D A

MONDAY, NOVEMBER 03, 2003

- | | |
|----------------------|---|
| 10.00 – 10.10 | - Welcome - Commonwealth Secretariat
Ms. C. Thompson-Barrow
Deputy Director, Head, Law and
Development Section, LCAD |
| 10.10 – 10.40 | - Opening Address - Hon AJ Nicholson
Attorney General & Minister of Justice of
Jamaica |
| 10.40 – 11.10 | - Coffee/Tea Break – “Meet and Greet” |



TUESDAY, NOVEMBER 04, 2003

- 10.00 – 11.00 - Model Bill on Electronic Transactions - Overview
by
Mr. Jeff Cumberbatch, Deputy Dean of the
Faculty of Law, UWI
- 11.00 – 11.15 - Coffee/Tea Break
- 11.15 – 12.15 - Open Discussions and Country Interventions
- 12.15 – 1.15 - Lunch
- 1.15 – 2.15 - Conclusions and Recommendations on Model
Bill on Electronic Transactions
- 2.15 – 2.30 - Coffee/Tea Break
- 2.30 – 3.30 - Continuation if necessary



WEDNESDAY, NOVEMBER 05, 2003

- 10.00 – 11.00 - Model Bill on Freedom of Information –
Overview by Dr Emmanuel Awuku,
Senior Programme Officer, LCAD**
- 11.00 – 11.15 - Coffee/Tea Break**
- 11.15 - 12.15 - Open Discussions and Country
Interventions**
- 12.15 – 1.15 - Lunch**
- 12.15 – 1.15 - Conclusions and Recommendations on the
Model Bill on Freedom of Information**
- 1.15 – 2.15 - Model Bill on Privacy –
Overview by Dr Emmanuel Awuku,
Senior Programme Officer, LCAD**
- 2.15 – 2.30 - Coffee/Tea Break**
- 2.30 – 3.30 - Open Discussions and Country
Interventions**
- 3.30 – 4.30 - Conclusions and Recommendations on
Model Bill on Privacy**



THURSDAY, NOVEMBER 06, 2003

- | | | |
|--|---|--|
| 10.00 – 11.00
Related | - | Model Bill on Computer and Computer
Crimes – Overview by Ms. Lucie Angers |
| 11.00 – 11.15 | - | Coffee/Tea Break |
| 11.15 - 12.15
Interventions | - | Open Discussions and Country |
| 12.15 – 1.15 | - | Lunch |
| 1.15 – 2.15 | - | Conclusions and Recommendations on the Model
Bill
on Computer and Computer Related Crimes |
| 2.15 – 2.30 | - | Coffee/Tea Break |
| 2.30 – 3.00 | - | Presentation by Lucie Angers:
“ E mail: Some Criminal Aspects” |



FRIDAY, NOVEMBER 07, 2003

- | | | |
|----------------------|----------|---|
| 10.00 - 11.00 | - | Revision of Conclusions and Recommendations of Workshop |
| 11.00 – 11.15 | - | Coffee/Tea Break |
| 11.15 – 12.15 | - | Finalisation of Conclusions and Recommendations of Workshop |
| 12.15 – 12.45 | - | Close of Meeting – Hon A J Nicholson
Attorney General of Jamaica |
| | - | Vote of Thanks
Mr Rogers W.O Okot Uma
GIDD, Commonwealth Secretariat |
| 1.00 | - | Lunch |