

# CYBER LEGISLATION: A MODEL LAW FOR THE SOUTH PACIFIC

*Nicola Scott\**

---

*The APT/ITU/PITA/Workshop on Principles of Cyber Legislation for the Pacific Region Conference in Auckland, New Zealand in 2007 was dedicated to discussing the need and options for cyber legislation in Pacific countries. Against the background of the many obstacles to the preparation of such legislation in small countries, it was suggested that the best way to create such a law was for a country to enact existing international Model Laws and to adapt other countries' national cyber related legislation where it was an appropriate precedent. It is the purpose of this paper to demonstrate one way in which that could be done.*

*Une partie des travaux de la conférence sur le 'Principe of Cyber legislation for the Pacific' organisée en 2007 sous les auspices de l'APT, de l'UIT, et de la PITA, a porté sur le bien-fondé de la mise en place d'un cadre juridique commun susceptible de régir le domaine des transmissions par voie électronique dans le Pacifique. Pour contourner les difficultés que pourraient rencontrer les petits Etats insulaires de cette région qui souhaiteraient se doter de pareille législation, l'idée retenue a été que dans un premier temps, les textes issus des conventions internationales ou les principales décisions de justice qui intéressent la matière soient simplement transposés dans leurs droits nationaux respectifs. Cet article s'intéresse aux mesures concrètes qu'il conviendrait de mettre en œuvre pour satisfaire à cet objectif.*

---

## **I INTRODUCTION**

Many of the countries of the South Pacific have legislation and policies addressing the issues of e-commerce and e-crime or are in the process of developing them. The Pacific island countries have, however, limited capacity to draft and enact technology and resource intensive policies and legislation. Further, for most Pacific island countries concerns relating to the internet or e-commerce are not a high priority when compared to domestic economic and political issues. There is also the problem of enforcement and of policing the internet and cyberspace. Creating a Cyberlaw Act is however not difficult if reference is made to the existing legislation of other countries and to

---

\* BA(Hons), LLB, Barrister and Solicitor of the High Court of New Zealand.

internationally developed Model Laws which can be adapted to suit a particular Pacific country's circumstances.

The areas for a cyberlaw would be spam; contracting in cyberspace including on line contracts, electronic signature and authentication, online payment and consumer protection; personal data protection including privacy and data security; intellectual property; regulating online content and cybercrime, including cybercrime and infrastructure protection; and disputes management. For these topics Model Laws could be the United Nations Convention on the Use of Electronic Communications in International Contracts 2005, the UNCITRAL<sup>1</sup> Model Law on Electronic Signatures 2001, the UNCITRAL Model Law on Electronic Commerce 1996, the US Children's Internet Protection Act, and the US Trademark Cyberpiracy Prevention Act 1999.

Attached to this paper is a Cyberlaw Bill which serves to indicate a model law that most Pacific island countries could enact. Its main feature is that it is compiled almost exclusively from international precedents. The Bill addresses various situations that arise in the information and communication technologies (ICT) context. It seeks to encompass the subject areas of e-transactions, cybercrime, data protection, and electronic signatures.<sup>2</sup> The Bill allows for the general body of rules dealing with cyber communication to be set out in one place, rather than in a number of Acts and regulations.<sup>3</sup>

The advent of globalisation has meant that countries are unable to deal individually with certain problems created by cross-border interaction. Cyberspace is one such matter. It cannot be contained by national boundaries, thus territorial controls to regulate the internet are limited due to the fact that one state alone cannot successfully control it.

Cyberspace is not a vacant space or the new wild-west frontier. It is highly controlled and increasingly regulated. It is controlled by humans: programmers, internet organisations and legislation. Legislation deals with people and property within a nation's jurisdiction. A government is able to regulate things within its power; legislation that extends beyond a nation's territory is of

---

1 UNCITRAL is the United Nations' Commission on International Trade Law.

2 Areas not covered in this Bill are intellectual property rights, infrastructure security, and spam. Spam was excluded because that is a subject area where several Pacific countries either already have legislation or have draft legislation.

3 In addition to enacting special legislation to take account of the special ICT needs of the 21<sup>st</sup> century the existing law can be extended to cover many aspects of cyber activity by the simple expedient of amendments to a country's Interpretation Act. Some countries have recent interpretation statutes but many have laws based on 19<sup>th</sup> century English precedents which will typically describe "document" as something written and in physical form. An amendment to such a definition can instantly extend all the law to documents that are electronic in form or produced electronically such as faxes and emails. Similarly, general rules about meetings that require physical presence can be amended to allow for formal meetings (and resolutions) to be conducted on the internet or by tele-conferencing.

little value as it cannot operate in another nation's jurisdiction. International co-operation is therefore an option that should be pursued in dealing with cyberlaw issues. The enactment of a Bill, such as the one presented here, in small states would ultimately make cyber legislation consistent throughout the whole Pacific region.

## **II MAKING CYBER LEGISLATION**

### **A Fundamental Rights**

The constitutional law of each country has to be taken into consideration when using or adapting a model law. Specifically, some of the constitutions of the Pacific region protect privacy<sup>4</sup> and freedom of expression<sup>5</sup>, and all of the Pacific countries except Niue have a constitution which guarantees fundamental rights and freedoms. These fundamental rights need to be considered when regulating the internet because the constitution is the supreme law. Any statute which introduces a Model Law must do so in a manner compatible with the constitution.

Constitutional rights may, for instance, place limitations on a government's ability to restrict internet communications. For instance if a government wanted the power to block electronic communications, the power would either have to be sparingly used and restricted to situations of public order and public emergency to avoid falling foul of the constitutional protection of freedom of expression, or the Constitution would have to be amended.

It is important to note, from the point of view of the use of precedents of other countries, that neither New Zealand nor Australia has entrenched rights and freedoms. The effect of this is that if the legislation of New Zealand or Australia were adopted by a Pacific country unchanged and without reference to the constitution of the adopting country some of the adopted legislation may be *ultra vires*.

### **B Resource Availability**

The resources available to each state to implement any Model Law and to fulfil specific obligations in the Model Law will vary. The small island states have relatively limited human resources and technology. Pacific countries, due to their small populations and limited commercial strength, are therefore constrained in their ability to control the internet. There is a need for policy makers to consider both human and technological resources that are available in a Pacific island country before deciding on how to legislate for cyber issues.<sup>6</sup>

---

4 Countries that protect or contain rights of privacy in their Constitution are for example: Fiji s 37, Kiribati s 3, Marshall Islands s 13, Papua New Guinea s 49.

5 Countries with freedom of expression provisions in their Constitution are the Cook Islands s 64, Kiribati ss 3 and 12, Marshall Islands art 2, Samoa s 13, Vanuatu ch 2 cl 5.

6 There is the potential to meet these difficulties by sharing resources in a Pacific regional group.

### *C Legislative Alternatives*

The main options for creating a cyberlaw text are (1) to draft one from scratch, (2) to implement a treaty, (3) to adapt legislation from another country's domestic legislation, or (4) to adopt a Model Law into domestic legislation.

In the countries of the South Pacific, drafting a new law from scratch is unlikely to be possible for resource reasons. Adapting legislation is less difficult than starting from scratch, nevertheless the legislation needs to be identified and then, because it is another country's domestic legislation, it needs to be reviewed to ensure that the provisions are of general application and not specific to the circumstances of the country of origin.

Having chosen the text, or method of creating a text, a decision must be taken on how to legislate that text: whether in one Act or Code, or by amending an existing Act or Regulation. This decision will be influenced substantially by any existing legislation on cyber matters and to a lesser extent by the legislative procedures of the country. The advantage of a single Act or Code is that the law will be in one place and consistent within itself.<sup>7</sup> Having several Acts runs the risk of having inconsistent cyber laws. Further, the grafting of major new rules into existing legislation is likely to lead to inconsistencies or omissions.

#### *1 Treaty*

The strongest form is to have a treaty and domestic legislation that implements the treaty. The treaty option has two immediate advantages: the law across several countries will be consistent, and the treaty will provide the implementing state with a ready-made text.

#### *2 Model Laws*

The next best system of ensuring international co-operation is to adopt a Model Law that has been prepared by a regional or international organisation. This is a relatively easy option once the relevant model has been identified. Model Laws come in various guises. They may be presented as such eg the UNCITRAL Model Law on Electronic Commerce, or in a form which sets out the objectives for legislating.<sup>8</sup>

If states adopt a model law, laws are harmonised and international trade is increased through the transparency of laws. Model Laws have the advantage for administrators and courts, of substantial commentaries and explanations.

---

7 For accessibility, legislation relating to ICT should be in a Code or in one Act, rather than inserted in, for example, a Companies Act where its existence would not be obvious.

8 Eg the EC Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (1995).

All the provisions in the draft Bill in the Appendix to this paper come from pre-existing texts.<sup>9</sup> The Model Laws which require little or no adaptation to the situation of the adopting country are included in Schedules to the Bill. Provisions which are adopted from other countries' domestic legislation or which require greater adaptation to the enacting state's situation have been included as Parts in the main body of the Bill.

#### ***D Drafting***

The physical presentation of the law can be in the form of an Act with specific Parts dealing with discrete subject-matters, or in the form of an Act whose main body is brief and declares various sets of rules to be law and then produces those sets of rules in separate schedules to the Act.

It is best to create an Act in Parts. If a specific Part is contentious it can be easily removed without affecting the overall Act; if a Part is unacceptable to a majority in Parliament, that Part can be removed from the Bill so as to allow the passage of the non-contentious Parts.

The attached Bill is premised on the idea that cyber legislation should be in a single document.<sup>10</sup>

### ***III THE SUBJECT AREAS***

#### ***A E-Contracts***

There are several models for e-transaction law. UNCITRAL has provided a code<sup>11</sup> which aims to equalise the treatment of online and offline forms of communication.

Some countries have already recognised and used the Model Laws or a version of them has been adopted into domestic legislation. For example, New Zealand and Australia have enacted legislation based on the UNCITRAL model. The New Zealand Electronic Transactions Act 2000 and Australia Electronic Transactions Act 1999 are based on the UNCITRAL Model Law on Electronic Commerce and UNCITRAL Model Law on Electronic Signatures.

New Zealand and Australia domestic privacy laws are consistent with the EC Directive.<sup>12</sup>

---

9 Eg the Computer Crimes Act 2003 of Tonga, the Telecommunications Act 2004 of Kiribati, The Wire Act 18 USC 1084 of the US, and the International Sales Contract Regulations 2001 of Alberta, Canada. The adoption of regional Acts is because these countries have similar resource and technological capabilities.

10 Achievement of that goal is compromised by the fact that some areas of cyber law have already been legislated, or are in the process of being legislated, in Pacific countries, for example spam.

11 I am not sure what this is in reference to – is it just the UNCITRAL Model Laws about contracts?

12 The United Kingdom's implementation of the EC Directive was by the Data Protection Act 1998. If used as an example for the Pacific, the Directive's basic principles should be implemented in a simplified form. NZ has the Privacy Act 1993 (and among other codes implemented under this Act, there is the Telecommunications Information Privacy Code 2003). NZ currently has a bill in the House to deal with some cross-border privacy issues – mainly arising from the internet. Australia has the Privacy Act 1988 (amended in 2000 largely due to the concern that its existing law was not consistent with the EC Directive

The main alternative to the UNCITRAL model is the EC Directive on certain legal aspects on information society services, in particular electronic commerce, in the Internal Market – Directive on Electronic Commerce. The Directive was introduced to clarify and harmonise the rules relating to on-line business.<sup>13</sup> The Directive includes requirements on:

- the information an on-line service provider must give a consumer;
- the information a consumer must have about the steps to take to conclude a contract on-line;
- the information that must be given about the sender, discounts, offers etc. in on-line advertising;
- ways to make it easier for internet users to protect themselves from unsolicited emails;
- the limitation of intermediate service providers' liability for unlawful information or activities they carry or store; and
- the national law that will apply to a cross-border transaction.

Other than in Australia and New Zealand, e-contract legislation in the Pacific is rare. Vanuatu is one country which has laws to reflect the 21<sup>st</sup> century situation. It has enacted an Electronic Transactions Act 2000 and the Companies (E-Commerce Amendment) Act 2000 to amend the Companies Act and the E-Business Act 2000.

### ***B Cybercrime***

Cybercrime deals with "an offence where a computer is used as a tool in the commission of an offence, as the target of an offence, or used as a storage device in the commission of an offence."<sup>14</sup> It is considered an international crime because there is strong potential for these crimes to have cross-border effects. The challenge for legislators is that the internet has features which favour criminal activity<sup>15</sup> – unregulated establishment of email sites and access to internet and email sites, anonymity, lack of security and public awareness, and lack of data.

Some types of criminal activity using internet and technology have been incorporated into general Acts. For example, section 249 of the New Zealand Crimes Act 1961 deals with accessing computer system for a dishonest purpose; Australia's Cybercrime Act 2001 incorporates many of the

---

and therefore that its opportunities in the global market could be jeopardised). The UK has also enacted the Freedom of Information Act 2000 and the Privacy and Electronic Communications [EC Directive] Regulations 2003.

13 Exceptions to this principle include contracts that involve the sale of land, and contracts of guarantee.

14 The Australasian Centre for Policing Research. See [http://www.acpr.gov.au/pdf/ACPR134\\_1.pdf](http://www.acpr.gov.au/pdf/ACPR134_1.pdf)

15 Conventional crimes that may be committed with the use of cyber technology include fraud, pornography and illegal internet gambling.

provisions of the European Convention on Cybercrime<sup>16</sup> and includes provisions on unauthorised access, modification or impairment with intent to commit a serious offence.<sup>17</sup>

### ***C Internet Pornography***

There is no international law on the distribution, purchase, or possession of internet pornography. Article 9 of the European Convention on Cybercrime requires parties of the Convention to adopt "legislative and other measures as may be necessary to establish as criminal offences under its domestic law" conducts of producing, offering or making available, distributing or transmitting, procuring, or possessing child pornography through a computer system. Section 70 of the Kiribati Telecommunications Act 2004 criminalises distribution and exhibition of obscene matter.<sup>18</sup>

In countries where some forms of pornography are legal, several commercial pornography sites have developed voluntary means of protection against access by children by restricting access to any pornographic content until a membership has been purchased using a credit card. This serves as both a way to collect payment and an age verification method since credit cards are not issued to minors.

### ***D Online Gambling***

Online gambling is both a means of recreation and entertainment and a source of export earnings. Online gambling generates billions of dollars annually but it also generates risks. It encourages compulsive gambling; it can involve illegal purposes such as money laundering; it is easily used for fraud;<sup>19</sup> credit card or account details may be vulnerable to capture, and funds vulnerable to theft by computer hackers; online gambling can be easily accessible to children.

The challenge faced by legislators when regulating online gambling is a difficult one because cyberspace knows no physical frontiers. There are also many difficulties in the enforcement of offences, for example the resources needed for locating, investigating, and prosecuting an online offender who is offshore are substantial. A great degree of surveillance is required. The enforcement resources of most Pacific nations are limited, and the capacity of police to detect and investigate sophisticated high technology crime is even more limited.

Regulation is important for consumer protection. This is no different from the regulation of "physical" casino gambling: to ensure the integrity of the market, to guarantee the probity of service providers.

---

16 Convention on Cybercrime, Council of Europe, 2001.

17 Australia's Cybercrime Act 2001, amending Criminal Code Act 1995, s 477.1.

18 "Matter" includes electronic reproduction.

19 For example the provider of online gambling services can take a punter's money and shut down failing to pay winnings.

The US Wire Act, 18 USC 1084 prohibits gamblers from using telephone facilities to receive bets or send gambling information. The Act prohibits not only the placing of bets but also the transmission of information assisting in the placing of bets or wagers on any sporting event or contests. This means that even a casino that does not actually take wagers from players can breach the Act.

The New Zealand Gambling Act 2003 restricts the operation of remote interactive gambling. The Act's definition of remote interactive gambling includes gambling at a distance using a communication device, like a website, text, telephone, television, radio, or other media.

Vanuatu Interactive Gaming Act 2000 approves interactive games (section 19), but requires the licensee's control systems be approved by the Regulator (section 20) and prohibits internet gambling by persons under 18 (section 18).

### ***E Critical Infrastructure Protection***

Certain national infrastructures are critical to the physical and economic security of a country. The systems and networks that comprise the critical infrastructure are essential to a country's stability. Critical infrastructure protection focuses on trying to secure and protect these systems and networks. Threats include equipment failures, human error, weather and other natural causes, physical attacks and cyber attacks.

Access to these interlinking systems can be managed through the internet from all over the world, blurring traditional borders. This interdependent and interrelated infrastructure is more vulnerable to physical and cyber disruptions because it has a complex system with single points of failure. (However, while single linear systems are highly vulnerable to single failures a non-linear system with multiple links could, potentially, sustain failures through re-routing systems.)

Critical infrastructure protection requires the development of national capability to identify and monitor the critical elements. It also needs to determine when and if the elements are under attack or disrupted by natural causes.

The infrastructure in a country includes systems and networks from major sectors such as:

- energy, including oil, natural gas and electric power;
- banking and finance;
- transportation, including air, surface and water transportation;
- water systems;
- government and private emergency services.

Computer offences provisions are designed to protect the security, integrity and reliability of computer data and electronic communications. The provisions present a strong deterrent to persons who engage in cybercrime activities.<sup>20</sup>

Australia's Cybercrime Act 2001 differentiates between serious computer offences and other computer crimes. The Act has extensive definitions<sup>21</sup> and provisions on unauthorised access, modification or impairment with intent to commit a serious offence; unauthorised modification of data to cause impairment; and unauthorised impairment of electronic communication. Definitions and provisions are also included in the Acts that refer to unauthorised access to, or modification of, restricted data; unauthorised impairment of data held on a computer disk; and possession or control of data with intent to commit a computer offence; producing, supplying or obtaining data with intent to commit a computer offence.

By contrast, Part II of the Tonga Computer Crimes Act 2003 deals with the computer offences in a more simplified way. It lists the following offences: illegal access, interfering with data, interfering with computer system, illegal interception of data, and illegal devices. Arguably, this is sufficient for Tonga. The Tonga Computer Crimes Act 2003 demonstrates that the Pacific island countries should look within the region for similar legislation rather than getting complicated and unworkable legislation from a metropolitan state.

#### ***F Spam***

The EU Directive on Privacy and Electronic Communications requires member states to take appropriate measures to ensure that unsolicited communications for purposes of direct marketing are not allowed without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications.<sup>22</sup>

New Zealand and Australia have adapted the EU Directive on Privacy and Electronic Communications into their domestic legislation: the Unsolicited Electronic Messages Act 2007 and the Spam Act 2003 respectively.

The Spam Act 2003 of Australia aims to reduce the amount of spam sourced in Australia, to reduce the volume of spam for end-users and to extend Australia's involvement in international anti-spam initiatives. The New Zealand Unsolicited Electronic Messages Act 2007 purports to promote a safer and more secure environment for the use of ICT in New Zealand; reduce impediments to the uptake and effective use of information and communications technologies by businesses and the

---

20 The Security Legislation Amendment (Terrorism) Act 2002 (Australia) makes specific reference to the concept of cyber-terrorism.

21 It also has provisions on intention, and provides for the situation of impossibility and attempt. See Australia's Cybercrime Act 2001, Sch 1 on amendments to Criminal Code Act 1995.

22 EU Directive on Privacy and Electronic Communications, art 13.

wider community in New Zealand; and reduce the costs to businesses and the wider community that arise from unsolicited commercial electronic messages.<sup>23</sup>

For Pacific island countries the New Zealand model will be better than the Australia one because it is simpler. Furthermore, Australia has a federal system, so adopting Australia's spam legislation involves more adaptation for Pacific island countries than using New Zealand's legislation on spam.<sup>24</sup>

#### ***IV IMPLEMENTING THE DRAFT BILL***

The references to Government officials in the Bill will vary depending on which Pacific country is enacting the Bill: References to "Cabinet making regulations" can be changed to reflect the body or person who has the authority to make regulations; References to the "Financial Secretary" are to the Head of the Government department responsible for Government finances; References to judges and courts are signalled where "[insert relevant judge or court]" appears. It is for the enacting state to decide what level of judge or court should be inserted. Government officials also need to decide upon the amount fined for particular offences. This is signalled where "[insert fine]" appears.

The ellipses which appear in the Schedules indicate those places where the Model Law has given a range of options which have not been reproduced in the Bill. The reason for the omission is that the options are mostly presented for metropolitan areas where complex cyberlaw systems already exist. Most are not relevant to the current Pacific systems. It is recommended that Pacific island countries should leave the options out of their domestic legislation for the present. As a country's systems develop any optional addition that becomes relevant can then be included in the law.

#### ***V CONCLUSION***

Digital globalisation establishes international connectivity in governmental, commercial and recreational areas. It affects people's everyday life and business, as well as society's law and order. The main areas of concern are electronic transactions, cybercrime, illegal online gambling and illegal internet pornography. The Pacific island countries need to legislate to enable people to fully embrace the opportunities that the technology offers to give them some protection from the criminal activities or commercial disputes which came with the opportunities.

A good way for Pacific nations to legislate is to adopt a Model Law. The Pacific nations have relatively limited resources, and adopting models enables legislation to be made without large resource costs. Furthermore, there is no boundary in cyberspace. Similar models will work well in

---

23 See New Zealand Unsolicited Electronic Messages Act 2007, s 3.

24 The Bill appended to this paper does not have provisions on spam because some Pacific island countries have existing or draft legislation on spam.

countries with similar cultural and economic backgrounds. A united approach, at least in the region, will reduce the possibility of loopholes, and ensure consistency of the law.

**APPENDIX**  
**CYBER LAW BILL**

**Explanatory Note**

The purpose of this Bill is to provide comprehensive legislation that addresses various situations arising from ICT use.

Part 1 of the Bill is introductory.

Part 2 of the Bill implements the UNCITRAL Model Law on Electronic Commerce and the UNCITRAL Model Law on Electronic Signatures.

Part 3 deals with cybercrime. It is adapted from the Computer Crimes Act 2003 (Tonga) which was based on the Convention on Cybercrime of the Council of Europe of 2001.

Part 4 deals with internet pornography. The precedent a provision is from the **Telecommunications Act 2004 (Kiribati)**.

Part 5 deals with Online Gambling and is adapted from the **Wire Act, 18 USC 1084 (USA)**.

Part 6 deals with Internet Sales Contracts and is based on the **Alberta Internet Sales Contract Regulations 2001 (Alberta)**.

PART 1	PART 5
PRELIMINARY	ONLINE GAMBLING
1 Title	22 Wagering information
PART 2 ELECTRONIC COMMERCE AND ELECTRONIC SIGNATURE	PART 6 INTERNET SALES CONTRACTS
2 Interpretation	23 Interpretation
3 Model laws to have force of law	24 Application
4 Application	25 Disclosure of information
PART 3 CYBERCRIME	26 Opportunity to accept or decline
5 Interpretation	27 Copy of internet sales contract
6 Jurisdiction	28 Cancellation of internet sales contract
7 Illegal access	29 Effect of cancellation
8 Interfering with data	30 Duty of supplier upon cancellation
9 Interfering with computer system	31 Application by supplier for relief
	32 Recovery for on cancellation under

10	Illegal interception of data	section 28
11	Illegal devices	33 Rights preserved
12	Search and seizure warrants	
13	Assisting police	PART 7
14	Protection of data	MISCELLANEOUS
15	Disclosure of traffic data	
16	Preservation of data	
17	Interception of electronic communications	
18	Interception of traffic data	
19	Evidence	
20	Confidentiality and limitation of liability	
PART 4		SCHEDULES
INTERNET PORNOGRAPHY		
21	Distribution and exhibition of obscene matter	

## PART 1

## PRELIMINARY

**1 Title**

This is the Cyber Law Act.

## PART 2

## ELECTRONIC COMMERCE AND ELECTRONIC SIGNATURES

**2 Interpretation**

In this Part –

"Director" means the public officer responsible for telecommunications;

"Electronic Commerce Law" means the UNCITRAL Model Law on Electronic Commerce of 12 June 1996 as set out in Schedule 1;

"Electronic Signatures Law" means the UNCITRAL Model Law on Electronic Signatures of 5 July 2001 as set out in Schedule 2.

**3 Model laws to have force of law**

Subject to this Act the Electronic Commerce Law and the Electronic Signatures Law are law in [enacting country].

#### 4 Application

- (1) The Electronic Commerce Law and the Electronic Signatures Law apply to every enactment that is part of the law of [enacting country] whether passed before or after the commencement of this Act.
- (2) The Electronic Commerce Law and the Electronic Signatures Law apply except to the extent that an enactment of [enacting country] provides otherwise.
- (3) The Electronic Commerce Law and the Electronic Signatures Law do not apply to –
  - (a) [List any relevant legislation].
  - (b) ...
- (4) The Electronic Commerce Law and the Electronic Signatures Law do not apply to provisions in enactments relating to -
  - (a) Notices that are required to be given to the public;
  - (b) Information that is required to be given in writing either in person or by registered post;
  - (c) Notices that are required to be attached to any thing or left or displayed in any place;
  - (d) Documents given on oath or affirmation;
  - (e) Powers of attorney;
  - (f) Testamentary instruments;
  - (g) Negotiable instruments;
  - (h) Instruments or any other documents presented to, deposited with, entered on the register or filed by, the Registrar of the [insert relevant court], the Registrar of Births and Deaths, or a Marriage Officer;
  - (i) Notices or certificates required to be given to a patient or proposed patient regarding assessment, treatments, alteration to treatments, or any review process;
  - (j) Requirements to produce or serve a warrant or other document that authorises –
    - (i) entry on premises; or
    - (ii) the search of any person, place, or thing; or
    - (iii) the seizure of any thing;
  - (k) The practice or procedure of the [insert relevant judge or court] except to the extent that rules of [insert relevant court] provide for the use of electronic technology.
- (5) For the purposes of article 7 of the Electronic Signatures Law is the Director,
  - (a) The person empowered
  - (b) the competent person is the Financial Secretary.
- (7) In article 12 of the Electronic Signatures Law "[enacting country eg Niue]" is "[the enacting State]".

PART 3  
CYBERCRIME

**5 Interpretation**

In this Part –

"computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include –

- (a) An automated typewriter or typesetter;
- (b) A portable hand-held calculator; or
- (c) A similar device which is non-programmable or which does not contain any data storage facility;
- (d) Such other device as the [Cabinet] may prescribe by regulation;

"computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a programme suitable to cause a computer system to perform a function;

"computer data storage medium" means any article or material such as a disk, from which information is capable of being reproduced, with or without the aid of any other article or device;

"computer system" means a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a programme, performs automatic processing of data or any other function;

"hinder", in relation to a computer system, means –

- (a) Cutting the electricity supply to a computer system;
- (b) Causing electromagnetic interference to a computer system;
- (c) Corrupting a computer system by any means; and
- (d) Inputting, deleting or altering computer data;

"seize" includes –

- (a) Make and retain a copy of computer data, including using on site equipment;
- (b) Render inaccessible, or remove, a computer, computer data in the accessed computer system; and
- (c) Take a printout of computer data;

"service provider" means –

- (a) a public or private entity that provides to users of its services the ability to communicate by means of a computer system; and
- (b) any other entity that processes or stores computer data on behalf of that entity or those users;

"traffic data" means computer data that relates to a communication by means of a computer system, and is generated by a computer system that is part of the chain of communication, and shows the communication's origin, destination, route, time, date, size, duration or the type of underlying services.

## **6 Jurisdiction**

- (1) A person who does an act outside [enacting country] which if done in [enacting country] would be an offence under this Part, shall be deemed to have committed the offence in [enacting country].
- (2) This Part shall apply as if, for the offence in question –
  - (a) The accused; or
  - (b) The computer, programme or data, was in [enacting country] at the material time.

## **7 Illegal access**

- (1) For the purposes of this section, a computer shall be treated as a "protected computer" if the person committing the offence knew, or ought reasonably to have known, that the computer or programme or data is used directly in connection with or necessary for –
  - (a) The security, defence or international relations of [enacting country];
  - (b) The existence or identity of a confidential source of information relating to the enforcement of a criminal law;
  - (c) The provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or
  - (d) The protection of public safety including system related to essential emergency services.
- (2) A person who wilfully, without lawful excuse, accesses any computer system commits an offence and shall be liable upon conviction to a fine not exceeding [insert fine] or imprisonment for a period not exceeding 2 years or to both.
- (3) A person who wilfully, without lawful excuse, accesses any protected computer commits an offence and shall be liable upon conviction to a fine not exceeding [insert fine] or to imprisonment for a period not exceeding 20 years or to both.

- (4) For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused has the requisite knowledge referred to in this section if there is, in respect of the computer, programme or data, an electronic or other warning exhibited to the accused stating that unauthorised access to that computer, programme or data is an offence.

#### **8 Interfering with data**

A person who, wilfully or recklessly without lawful excuse –

- (a) Destroys or alters data;
- (b) Renders data meaningless, useless or ineffective;
- (c) Obstructs, interrupts or interferes with the lawful use of data;
- (d) Obstructs, interrupts or interferes with any person in the lawful use of data; or
- (e) Denies access to data to any person entitled to it; commits an offence and shall be liable upon conviction, to a fine not exceeding [insert fine] or to imprisonment for a period not exceeding 2 years or to both.

#### **9 Interfering with computer system**

A person who wilfully or recklessly, without lawful excuse –

- (a) Hinders or interferes with the functioning of a computer system; or
- (b) Hinders or interferes with a person who is lawfully using or operating a computer system,

commits an offence and shall be liable upon conviction to a fine not exceeding [insert fine] or imprisonment for a period not exceeding 1 year or to both.

#### **10 Illegal interception of data**

A person who, wilfully without lawful excuse, intercepts by technical means –

- (a) Any transmission to, from or within a computer system; or
- (b) Electromagnetic emissions from a computer system that are carrying computer data,

commits an offence and shall be liable upon conviction, to a fine not exceeding [insert fine] or imprisonment for a period not exceeding 1 year or to both.

#### **11 Illegal devices**

(1) A person who:

- (a) Wilfully or recklessly, without lawful excuse, produces, sells, procures for use, imports, exports, distributes or makes available –
  - (i) a device, including a computer programme, that is designed or adapted for the purpose of committing an offence under sections 7, 8, 9, or 10; or

(ii) a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed; with the intent that it be used by any person for the purpose of committing an offence under sections 7, 8, 9, or 10; or

(b) Has an item mentioned in subparagraph (i) or (ii) in his possession with the intent that it be used by any person for the purpose of committing an offence under sections 7, 8, 9, or 10,

commits an offence and shall be liable upon conviction to a fine not exceeding [insert fine] or imprisonment for a period not exceeding 4 years or to both.

(2) A person who possesses more than one item mentioned in subsection (1)(i) or (ii), is deemed to possess the item with the intent that it be used by any person for the purpose of committing an offence under sections 7, 8, 9, or 10.

## 12 Search and seizure warrants

(1) If a [insert relevant judge or court] is satisfied on sworn evidence that there are reasonable grounds to suspect that there may be in a place a computer, computer system, computer data or data storage medium which –

- (a) May be material evidence in proving an offence; or
- (b) Has been acquired by a person as a result of an offence;

the [insert relevant judge or court] may issue a warrant authorizing any constable, with such assistance as may be necessary, to enter the place to search and seize the computer, computer system, computer data or data storage medium.

(2) Any person who makes a search or seizure under this section, shall at the time or as soon as practicable –

- (a) Make a list of what has been seized, with the date and time of seizure; and
- (b) Give a copy of that list to —
  - (i) the occupier of the premises; or
  - (ii) the person in control of the computer system.

(3) Subject to subsection (4), on request, any constable or another authorized person shall –

- (a) Permit a person who had the custody or control of the computer system, or someone acting on their behalf to access and copy computer data on the system; or
- (b) Give the person a copy of the computer data.

- (4) The constable or another authorized person may refuse to give access or provide copies if he has reasonable grounds for believing that giving the access, or providing the copies may –
- (a) Constitute a criminal offence; or
  - (b) Prejudice –
    - (i) the investigation in connection with which the search was carried out;
    - (ii) another ongoing investigation; or
    - (iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations.

### **13 Assisting police**

- (1) A person who is in possession or control of a computer, computer system, computer data or data storage medium that is the subject of a search under section 12 shall permit, and assist if required, the person making the search to –
- (a) Access and use a computer system or computer data storage medium to search any computer data available to or in the system;
  - (b) Obtain and copy that computer data;
  - (c) Use equipment to make copies; and
  - (d) Obtain an intelligible output from a computer system in a format that can be read.
- (2) A person who fails without lawful excuse to permit or assist a person acting under a search warrant commits an offence and shall be liable upon conviction to a fine not exceeding [insert fine] or imprisonment for a period not exceeding 2 years or to both.

### **14 Production of data**

A [insert relevant judge or court] on application by a constable that specified computer data, or a printout or other information is reasonably required for the purpose of a criminal investigation or criminal proceedings, may order –

- (a) A person in control of a computer system to produce from the system specified computer data or a printout or other intelligible output of that data;
- (b) An internet service provider to produce information about persons who subscribe to or otherwise use the service; and
- (c) A person who has access to a specified computer system process to compile specified computer data from the system and give it to a specified person.

**15 Disclosure of traffic data**

Where a [insert relevant judge or court] is satisfied on the basis of an application by a constable that specified data stored in a computer system is reasonably required for the purpose of a criminal investigation or criminal proceedings, the [insert relevant judge or court] may order that a person in control of the computer system disclose sufficient traffic data about a specified communication to identify –

- (a) The service providers; and
- (b) The path through which the communication was transmitted.

**16 Preservation of data**

(1) Where a constable is satisfied that –

- (a) Data stored in a computer system is reasonably required for the purpose of a criminal investigation; and
- (b) There is a risk that the data may be destroyed or rendered inaccessible;

the constable may, by written notice given to a person in control of the computer system, require the person to ensure that the data specified in the notice be preserved for a period of up to 7 days as specified in the notice.

(2) The [insert relevant judge or court] may upon application authorise an extension not exceeding 14 days.

**17 Interception of electronic communications**

Where a [insert relevant judge or court] is satisfied on the evidence that there are reasonable grounds to suspect that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the [insert relevant judge or court] may –

- (a) Order an internet service provider to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or
- (b) Authorise any constable to collect or record that data through application of technical means.

**18 Interception of traffic data**

(1) Where a constable is satisfied that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the constable may, by written notice given to a person in control of such data, request that person to –

- (a) Collect or record traffic data associated with a specified communication during a specified period; and
  - (b) Permit and assist a specified constable to collect or record that data.
- (2) Where a [insert relevant judge or court] is satisfied on the evidence that there are reasonable grounds to suspect that traffic data is reasonably required for the purposes of a criminal investigation, the [insert relevant judge or court] may authorise any constable to collect or record traffic data associated with a specified communication during a specified period through application of technical means.

#### **19 Evidence**

In proceedings for an offence under this Act the fact that –

- (a) It is alleged that an offence of interfering with a computer system has been committed; and
  - (b) Evidence has been generated from that computer system;
- does not of itself prevent that evidence from being admitted.

#### **20 Confidentiality and limitation of liability**

(1) An internet service provider who without lawful authority discloses –

- (a) The fact that an order under sections 14, 15, 16, 17, or 18 has been made;
- (b) Anything done under the order; or
- (c) Any data collected or recorded under the order;

commits an offence and shall be liable upon conviction to a fine not exceeding [insert fine] or imprisonment for a period not exceeding 10 years or to both.

(2) An internet service provider shall not be liable under any law for the disclosure of any data or other information that a person discloses under sections 14, 15, 16, 17, or 18.

### PART 4

#### INTERNET PORNOGRAPHY

#### **21 Distribution and exhibition of obscene matter**

(1) In this Part -

"distribute" means transfer possession of, with or without payment or other reward;

"knowingly" means being aware of the character of the matter;

"matter" -

- (a) means any recording, pictorial representation, figure, transcription, printed or written material, mechanical, chemical, electrical, or electronic reproduction, or other article, equipment, machine, or material, and includes but is not limited to any book, magazine, newspaper, picture, drawing, photograph, motion picture, statue, film, filmstrip, negative, slide, photocopy, videotape, video laser disc, computer hardware, computer software, computer floppy disc, data storage medium, CD-ROM, computer-generated image, or computer-generated equipment, and
- (b) includes any live or recorded telephone message if transmitted, disseminated, or distributed as part of a commercial transaction;

"obscene matter" means matter which, applying contemporary [enacting country] standards, appeals to the prurient interest, depicts or describes sexual conduct in a patently offensive way, and, taken as a whole, lacks serious literary, artistic, or scientific value.

- (2) In determining whether matter lacks serious literary, artistic, or scientific value, the fact that the defendant knew that the matter depicted persons under the age of 16 years engaged in sexual conduct shall be taken into account.
- (3) Every person who knowingly sends or causes to be sent, or brings or causes to be brought, into [enacting country] for distribution, or who in [enacting country] possesses, prepares, publishes, produces, develops, duplicates, or prints, with intent to distribute or to exhibit to others, or who offers to distribute, distributes, or exhibits to others, any obscene matter, commits an offence and shall be liable on conviction to a fine not exceeding [insert fine] and imprisonment for a term not exceeding 2 years or both.

## PART 5

### ONLINE GAMBLING

#### **22 Transmission of wagering information**

- (1) A person who, being engaged in the business of betting or wagering, knowingly uses a wire communication facility for the transmission in commerce of bets or wagers or information assisting in the placing of bets or wagers on any sporting event or contest, or for the transmission of a wire communication which entitles the recipient to receive money or credit as a result of bets or wagers, or for information assisting in the placing of bets or wagers, shall be liable on conviction to a fine not exceeding [insert fine] or imprisoned for a term not exceeding 2 years or both.
- (2) Nothing in this section shall prevent the transmission in interstate or foreign commerce of information for use in news reporting of sporting events or contests, or for the transmission of information assisting in the placing of bets or wagers on a sporting event

or contest from a foreign country where betting on that sporting event or contest is legal into a foreign country in which such betting is legal.

- (3) When a person is notified in writing by the Director, that any facility furnished by it is being used or will be used for the purpose of transmitting or receiving gambling information it shall discontinue or refuse, the leasing, furnishing, or maintaining of such facility, after reasonable notice to the subscriber.

## PART 6

### INTERNET SALES CONTRACTS

#### **23 Interpretation**

In this Part –

- (a) "consumer" means an individual who receives or has the right to receive goods or services from a supplier as a result of a purchase, lease or other arrangement;
- (b) "consumer transaction" means the supply of goods or services by a supplier to a consumer as a result of a purchase, lease or other arrangement;
- (c) "internet" means the decentralised global network connecting networks of computers and similar devices to each other for the electronic exchange of information using standardized communication protocols;
- (d) "internet sales contract" means a consumer transaction formed by text-based internet communications;
- (e) "services" means any services offered or provided primarily for personal, family or household purposes;
- (f) "supplier" means a person who, in the course of the person's business, provides goods or services to consumers.

#### **24 Application**

This Part does not apply to goods and services that are immediately downloaded or accessed using the internet.

#### **25 Disclosure of information respecting internet sales contract**

Before entering into an internet sales contract with a consumer, a supplier shall disclose the information prescribed in Schedule 3.

#### **26 Express opportunity to accept or decline internet sales contract**

A supplier shall provide the consumer with an express opportunity to accept or decline the internet sales contract and to correct errors immediately before entering into it.

**27 Copy of internet sales contract**

- (1) A supplier shall provide a consumer who enters into an internet sales contract with a copy of the contract in writing or electronic form within 15 days after the contract is entered into.
- (2) A copy of the internet sales contract shall include the requirements prescribed by Schedule 3.
- (3) For the purposes of subsection (1), a supplier is considered to have provided a consumer with a copy of the internet sales contract if the copy is sent or otherwise provided in accordance with Schedule 3.

**28 Cancellation of internet sales contract**

A consumer may cancel an internet sales contract under the circumstances described in Schedule 3.

**29 Effect of cancellation**

- (1) Cancellation of an internet sales contract under section 28 operates to cancel the contract as if the contract had never existed.
- (2) Cancellation of an internet sales contract under section 28 also operates to cancel –
  - (a) Any related consumer transaction;
  - (b) Any guarantee given in respect of consideration payable under the contract; and
  - (c) Any security given by a consumer or a guarantor in respect of consideration payable under the contract,as if the contract had never existed.
- (3) Where credit is extended or arranged by the supplier, the credit contract is conditional on the internet sales contract whether or not the credit contract is a part of or attached to the internet sales contract and, where the internet sales contract is cancelled, that cancellation has the effect of cancelling the credit contract as if the internet sales contract had never existed.

**30 Duty of supplier upon cancellation**

- (1) Where an internet sales contract is cancelled under section 28, a supplier shall, within fifteen days from the date of cancellation, refund to a consumer all consideration paid by the consumer under the contract and any related consumer transaction, whether paid to the supplier or another person.
- (2) Where goods are delivered to a consumer under an internet sales contract that is cancelled under section 28, the consumer shall, within fifteen days from the date of cancellation or

delivery of the goods, whichever is later, return the goods to the supplier unused and in the same condition in which they were delivered.

- (3) A consumer may return the goods under subsection (2) by any method that provides the consumer with confirmation of delivery to the supplier.
- (4) The supplier shall accept a return of goods by a consumer under subsection (2).
- (5) The supplier is responsible for the reasonable cost of returning goods under subsection (2).
- (6) Goods that are returned by the consumer under subsection (2) otherwise than by personal delivery are deemed for the purposes of that subsection to have been returned when sent by the consumer to the supplier.
- (7) Any breach of the consumer's obligations under this section is actionable by the supplier as a breach of statutory duty.

### **31 Application by supplier for relief**

A supplier may make an application to the [insert relevant judge or court] claiming that it would be inequitable for an internet sales contract to be cancelled under section 28 and the court may, upon the application, make any order it considers appropriate.

### **32 Recovery of consideration where cancellation under section 28**

Where a consumer has cancelled an internet sales contract under section 28 and the supplier has not refunded all of the consideration within the fifteen days referred to in section 30, the consumer may recover the consideration from the supplier as an action in debt.

### **33 Rights preserved**

The rights of a buyer or borrower under this Part are in addition to any rights of the buyer or borrower under any other Act or by the operation of law and nothing in this Part shall be construed to derogate from such rights.

## **PART 7**

### **MISCELLANEOUS**

### **34 Regulations**

[Cabinet] may make such regulations as it thinks fit for the purposes of this Act and in such regulations provide for the taking of fees, the imposing of charges, prescribe offences, and the imposition of penalties for contravention of regulations.

**SCHEDULES****SCHEDULE 1****UNCITRAL Model Law on Electronic Commerce****Part one. Electronic commerce in general****CHAPTER I. GENERAL PROVISIONS***Article 1. Sphere of application*

This Law applies to any kind of information in the form of a data message used in the context of commercial activities.

The term "commercial" should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include, but are not limited to, the following transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road.

*Article 2. Definitions*

For the purposes of this Law:

(a) "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;

(b) "Electronic data interchange (EDI)" means the electronic transfer from computer to computer of information using an agreed standard to structure the information;

(c) "Originator" of a data message means a person by whom, or on whose behalf, the data message purports to have been sent or generated prior to storage, if any, but it does not include a person acting as an intermediary with respect to that data message;

(d) "Addressee" of a data message means a person who is intended by the originator to receive the data message, but does not include a person acting as an intermediary with respect to that data message;

(e) "Intermediary", with respect to a particular data message, means a person who, on behalf of another person, sends, receives or stores that data message or provides other services with respect to that data message;

(f) "Information system" means a system for generating, sending, receiving, storing or otherwise processing data messages.

*Article 3. Interpretation*

(1) In the interpretation of this Law, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith.

(2) Questions concerning matters governed by this Law which are not expressly settled in it are to be settled in conformity with the general principles on which this Law is based.

*Article 4. Variation by agreement*

(1) As between parties involved in generating, sending, receiving, storing or otherwise processing data messages, and except as otherwise provided, the provisions of chapter III may be varied by agreement.

(2) Paragraph (1) does not affect any right that may exist to modify by agreement any rule of law referred to in chapter II.

CHAPTER II. APPLICATION OF LEGAL REQUIREMENTS TO DATA MESSAGES

*Article 5. Legal recognition of data messages*

Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

*Article 5 bis. Incorporation by reference*

Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is not contained in the data message purporting to give rise to such legal effect, but is merely referred to in that data message.

*Article 6. Writing*

(1) Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.

(3) ...

*Article 7. Signature*

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) ...

*Article 8. Original*

(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:

(a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

(b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.

(3) For the purposes of subparagraph (a) of paragraph (1):

(a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

(4) ...

*Article 9. Admissibility and evidential weight of data messages*

(1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:

(a) on the sole ground that it is a data message; or,

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.

*Article 10. Retention of data messages*

(1) Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:

(a) the information contained therein is accessible so as to be usable for subsequent reference; and

(b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.

(2) An obligation to retain documents, records or information in accordance with paragraph (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

(3) A person may satisfy the requirement referred to in paragraph (1) by using the services of any other person, provided that the conditions set forth in subparagraphs (a), (b) and (c) of paragraph (1) are met.

CHAPTER III. COMMUNICATION OF DATA MESSAGES

*Article 11. Formation and validity of contracts*

(1) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.

(2) ...

*Article 12. Recognition by parties of data messages*

(1) As between the originator and the addressee of a data message, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

(2) ...

*Article 13. Attribution of data messages*

- (1) A data message is that of the originator if it was sent by the originator itself.
- (2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:
  - (a) by a person who had the authority to act on behalf of the originator in respect of that data message; or
  - (b) by an information system programmed by, or on behalf of, the originator to operate automatically.
- (3) As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if:
  - (a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or
  - (b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.
- (4) Paragraph (3) does not apply:
  - (a) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or
  - (b) in a case within paragraph (3)(b), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.
- (5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.
- (6) The addressee is entitled to regard each data message received as a separate data message and to act on that assumption, except to the extent that it duplicates another data message and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was a duplicate.

*Article 14. Acknowledgement of receipt*

(1) Paragraphs (2) to (4) of this article apply where, on or before sending a data message, or by means of that data message, the originator has requested or has agreed with the addressee that receipt of the data message be acknowledged.

(2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by

(a) any communication by the addressee, automated or otherwise, or

(b) any conduct of the addressee

sufficient to indicate to the originator that the data message has been received.

(3) Where the originator has stated that the data message is conditional on receipt of the acknowledgement, the data message is treated as though it has never been sent, until the acknowledgement is received.

(4) Where the originator has not stated that the data message is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator:

(a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

(b) if the acknowledgement is not received within the time specified in subparagraph (a), may, upon notice to the addressee, treat the data message as though it had never been sent, or exercise any other rights it may have.

(5) Where the originator receives the addressee's acknowledgement of receipt, it is presumed that the related data message was received by the addressee. That presumption does not imply that the data message corresponds to the message received.

(6) Where the received acknowledgement states that the related data message met technical requirements, either agreed upon or set forth in applicable standards, it is presumed that those requirements have been met.

(7) Except in so far as it relates to the sending or receipt of the data message, this article is not intended to deal with the legal consequences that may flow either from that data message or from the acknowledgement of its receipt.

*Article 15. Time and place of dispatch and receipt of data messages*

(1) Unless otherwise agreed between the originator and the addressee, the dispatch of a data message occurs when it enters an information system outside the control of the originator or of the person who sent the data message on behalf of the originator.

(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows:

(a) if the addressee has designated an information system for the purpose of receiving data messages, receipt occurs:

- (i) at the time when the data message enters the designated information system; or
- (ii) if the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is retrieved by the addressee;

(b) if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.

(3) Paragraph (2) applies notwithstanding that the place where the information system is located may be different from the place where the data message is deemed to be received under paragraph (4).

(4) Unless otherwise agreed between the originator and the addressee, a data message is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business. For the purposes of this paragraph:

(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business;

(b) if the originator or the addressee does not have a place of business, reference is to be made to its habitual residence.

(5) ...

**Part two. Electronic commerce in specific areas**

## CHAPTER I. CARRIAGE OF GOODS

*Article 16. Actions related to contracts of carriage of goods*

Without derogating from the provisions of part one of this Law, this chapter applies to any action in connection with, or in pursuance of, a contract of carriage of goods, including but not limited to:

- (a) (i) furnishing the marks, number, quantity or weight of goods;
- (ii) stating or declaring the nature or value of goods;
- (iii) issuing a receipt for goods;
- (iv) confirming that goods have been loaded;
  
- (b) (i) notifying a person of terms and conditions of the contract;
- (ii) giving instructions to a carrier;
  
- (c) (i) claiming delivery of goods;
- (ii) authorizing release of goods;
- (iii) giving notice of loss of, or damage to, goods;
  
- (d) giving any other notice or statement in connection with the performance of the contract;
  
- (e) undertaking to deliver goods to a named person or a person authorized to claim delivery;
  
- (f) granting, acquiring, renouncing, surrendering, transferring or negotiating rights in goods;
  
- (g) acquiring or transferring rights and obligations under the contract.

*Article 17. Transport documents*

(1) Subject to paragraph (3), where the law requires that any action referred to in article 16 be carried out in writing or by using a paper document, that requirement is met if the action is carried out by using one or more data messages.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for failing either to carry out the action in writing or to use a paper document.

(3) If a right is to be granted to, or an obligation is to be acquired by, one person and no other person, and if the law requires that, in order to effect this, the right or obligation must be conveyed to that person by the transfer, or use of, a paper document, that requirement is met if the right or obligation is conveyed by using one or more data messages, provided that a reliable method is used to render such data message or messages unique.

(4) For the purposes of paragraph (3), the standard of reliability required shall be assessed in the light of the purpose for which the right or obligation was conveyed and in the light of all the circumstances, including any relevant agreement.

(5) Where one or more data messages are used to effect any action in subparagraphs (f) and (g) of article 16, no paper document used to effect any such action is valid unless the use of data messages has been terminated and replaced by the use of paper documents. A paper document issued in these circumstances shall contain a statement of such termination. The replacement of data messages by paper documents shall not affect the rights or obligations of the parties involved.

(6) If a rule of law is compulsorily applicable to a contract of carriage of goods which is in, or is evidenced by, a paper document, that rule shall not be inapplicable to such a contract of carriage of goods which is evidenced by one or more data messages by reason of the fact that the contract is evidenced by such data message or messages instead of by a paper document.

(7) ...

## SCHEDULE 2

### UNCITRAL Model Law on Electronic Signatures (2001)

#### *Part One*

#### *Article 1. Sphere of application*

This Law applies where electronic signatures are used in the context of commercial activities. It does not override any rule of law intended for the protection of consumers.

....

The term "commercial" should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include, but are not limited to, the following transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing;

banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road.

*Article 2. Definitions*

For the purposes of this Law:

(a) "Electronic signature" means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message;

(b) "Certificate" means a data message or other record confirming the link between a signatory and signature creation data;

(c) "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy; and acts either on its own behalf or on behalf of the person it represents;

(d) "Signatory" means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents;

(e) "Certification service provider" means a person that issues certificates and may provide other services related to electronic signatures;

(f) "Relying party" means a person that may act on the basis of a certificate or an electronic signature.

*Article 3. Equal treatment of signature technologies*

Nothing in this Law, except article 5, shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements referred to in article 6, paragraph 1, or otherwise meets the requirements of applicable law.

*Article 4. Interpretation*

1. In the interpretation of this Law, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith.

2. Questions concerning matters governed by this Law which are not expressly settled in it are to be settled in conformity with the general principles on which this Law is based.

*Article 5. Variation by agreement*

The provisions of this Law may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under applicable law.

*Article 6. Compliance with a requirement for a signature*

1. Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for

which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

2. Paragraph 1 applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:

(a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and

(d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

4. Paragraph 3 does not limit the ability of any person:

(a) To establish in any other way, for the purpose of satisfying the requirement referred to in paragraph 1, the reliability of an electronic signature; or

(b) To adduce evidence of the non-reliability of an electronic signature.

5. ...

#### *Article 7. Satisfaction of article 6*

1. [Any person, organ or authority, whether public or private, specified by the enacting State as competent] may determine which electronic signatures satisfy the provisions of article 6 of this Law.

2. Any determination made under paragraph 1 shall be consistent with recognized international standards.

3. Nothing in this article affects the operation of the rules of private international law.

#### *Article 8. Conduct of the signatory*

1. Where signature creation data can be used to create a signature that has legal effect, each signatory shall:

(a) Exercise reasonable care to avoid unauthorized use of its signature creation data;

(b) Without undue delay, utilize means made available by the certification service provider pursuant to article 9 of this Law, or otherwise use reasonable efforts, to notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if:

- (i) The signatory knows that the signature creation data have been compromised; or
- (ii) The circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised;

(c) Where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the certificate throughout its life cycle or that are to be included in the certificate.

2. A signatory shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1.

*Article 9. Conduct of the certification service provider*

1. Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall:

(a) Act in accordance with representations made by it with respect to its policies and practices;

(b) Exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle or that are included in the certificate;

(c) Provide reasonably accessible means that enable a relying party to ascertain from the certificate:

- (i) The identity of the certification service provider;
- (ii) That the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;
- (iii) That signature creation data were valid at or before the time when the certificate was issued;

(d) Provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise:

- (i) The method used to identify the signatory;

- (ii) Any limitation on the purpose or value for which the signature creation data or the certificate may be used;
- (iii) That the signature creation data are valid and have not been compromised;
- (iv) Any limitation on the scope or extent of liability stipulated by the certification service provider;
- (v) Whether means exist for the signatory to give notice pursuant to article 8, paragraph 1 (b), of this Law;
- (vi) Whether a timely revocation service is offered;

(e) Where services under subparagraph (d) (v) are offered, provide a means for a signatory to give notice pursuant to article 8, paragraph 1 (b), of this Law and, where services under subparagraph (d) (vi) are offered, ensure the availability of a timely revocation service;

(f) Utilize trustworthy systems, procedures and human resources in performing its services.

2. A certification service provider shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1.

#### *Article 10. Trustworthiness*

For the purposes of article 9, paragraph 1 (f), of this Law in determining whether, or to what extent, any systems, procedures and human resources utilized by a certification service provider are trustworthy, regard may be had to the following factors:

- (a) Financial and human resources, including existence of assets;
- (b) Quality of hardware and software systems;
- (c) Procedures for processing of certificates and applications for certificates and retention of records;
- (d) Availability of information to signatories identified in certificates and to potential relying parties;
- (e) Regularity and extent of audit by an independent body;
- (f) The existence of a declaration by the State, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing; or
- (g) Any other relevant factor.

#### *Article 11. Conduct of the relying party*

A relying party shall bear the legal consequences of its failure:

- (a) To take reasonable steps to verify the reliability of an electronic signature; or
- (b) Where an electronic signature is supported by a certificate, to take reasonable steps:
  - (i) To verify the validity, suspension or revocation of the certificate; and
  - (ii) To observe any limitation with respect to the certificate.

*Article 12. Recognition of foreign certificates and electronic signatures*

1. In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had:

(a) To the geographic location where the certificate is issued or the electronic signature created or used; or

(b) To the geographic location of the place of business of the issuer or signatory.

2. A certificate issued outside *[the enacting State]* shall have the same legal effect in *[the enacting State]* as a certificate issued in *[the enacting State]* if it offers a substantially equivalent level of reliability.

3. An electronic signature created or used outside *[the enacting State]* shall have the same legal effect in *[the enacting State]* as an electronic signature created or used in *[the enacting State]* if it offers a substantially equivalent level of reliability.

4. In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of paragraph 2 or 3, regard shall be had to recognized international standards and to any other relevant factors.

5. Where, notwithstanding paragraphs 2, 3 and 4, parties agree, as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law.

**SCHEDULE 3**

**1 Disclosure of information**

A supplier shall disclose the following information to a consumer before entering into an internet sales contract with the consumer –

- (a) The supplier's name and, if different, the name under which the supplier carries on business;
- (b) The supplier's business address and, if different, the supplier's mailing address;

- (c) The supplier's telephone number and, if available, the supplier's e-mail address and facsimile number;
- (d) A fair and accurate description of the goods or services being sold to the consumer, including any relevant technical or system specifications;
- (e) An itemized list of the price of the goods or services being sold to the consumer and any associated costs payable by the consumer, including taxes and shipping charges;
- (f) A description of any additional charge that may apply to the contract, such as customs duties and brokerage fees, the amount of which cannot reasonably be determined by the supplier;
- (g) The total amount of the contract, or, where the goods or services are being purchased over an indefinite period, the amount of the periodic payments under the contract;
- (h) The currency in which amounts owing under the contract are payable;
- (i) The terms, conditions and method of payment;
- (j) The date when the goods are to be delivered or the services are to begin;
- (k) The supplier's delivery arrangements, including the identity of the shipper, the mode of transportation and the place of delivery;
- (l) The supplier's cancellation, return, exchange and refund policies, if any; and
- (m) Any other restrictions, limitations or conditions of purchase that may apply.

## **2 Information considered disclosed**

A supplier is considered to have disclosed to a consumer the information required to be disclosed in section 1 if –

- (a) The information is prominently displayed in a clear and comprehensible manner; and
- (b) The consumer is able to retain or print the information.

## **3 Content and delivery of internet sales contract**

- (1) A copy of an internet sales contract provided by a supplier shall include –
  - (a) The information required by section 1;
  - (b) The consumer's name or unique identifier; and
  - (c) The date the contract was entered into.
- (2) A copy of an internet sales contract provided by a supplier shall be –

- (a) Sent by e-mail to the e-mail address provided by the consumer to the supplier for the provision of information related to the contract;
- (b) Sent by facsimile to the facsimile number provided by the consumer to the supplier for the provision of information related to the contract;
- (c) Mailed or delivered to an address provided by the consumer to the supplier for the provision of information related to the contract; or
- (d) Provided to the consumer in any other manner by which the supplier can prove that the consumer has received the copy.

#### **4 Cancellation of internet sales contract**

- (1) A consumer may cancel an internet sales contract –
  - (a) At any time from the date the contract is entered into until 7 days after the consumer receives a copy of the contract if –
    - (i) the supplier did not disclose to the consumer the information in accordance with this Schedule,
    - (ii) the supplier did not provide the consumer with an express opportunity to accept or decline the contract and to correct errors in accordance with this Schedule;
  - (b) Within 30 days from the date the contract is entered into if the supplier does not provide the consumer with a copy of the contract in accordance with this Schedule;
  - (c) At any time before delivery of the goods or the commencement of the services under the contract if the delivery date or commencement date is specified in the contract and –
    - (i) in the case of goods, the supplier does not deliver the goods within 30 days from the delivery date specified in the contract or another delivery date agreed on by the consumer and the supplier, either in writing or in electronic form,
    - (ii) in the case of transportation, travel or accommodation services, the supplier does not begin the services on the commencement date specified in the contract or another commencement date agreed on by the consumer and the supplier, either in writing or in electronic form, or
    - (iii) in the case of services, other than those specified in paragraph (ii), the supplier does not begin the services within 30 days from the commencement date specified in the contract or another commencement date agreed on by the consumer and the supplier, either in writing or in electronic form;

- (d) At any time before the delivery of the goods or the commencement of the services under the contract, if the delivery date or commencement date is not specified in the internet sales contract and if the supplier does not deliver the goods or begin the services within 30 days from the date the contract is entered into.
- (2) For the purposes of subsection (1), a supplier is considered to have delivered the goods under an internet sales contract if –
    - (a) Delivery was attempted but was refused by the consumer at the time that the delivery was attempted; or
    - (b) Delivery was attempted but was not made because no person was available to accept delivery for the consumer on the day for which reasonable notice was given to the consumer that the goods were available to be delivered.
  - (3) For the purposes of subsection (1), a supplier is considered to have begun the services under an internet sales contract if –
    - (a) Commencement was attempted but was refused by the consumer at the time that commencement was attempted; or
    - (b) Commencement was attempted but did not occur because no person was available to enable the services to begin on the day for which reasonable notice was given to the consumer that the services were available to begin.

## **5 Notification of cancellation**

- (1) A consumer may notify a supplier of cancellation of their internet sales contract in any manner or form that indicates the consumer's intent to cancel the contract.
- (2) Notification under subsection (1) may be given to the supplier by any means including, but not limited to, personal service, registered mail, telephone, courier, facsimile and e-mail, and when given other than by personal service, is deemed to be given when sent.

