GLACY
Global Action on Cybercrime
Action globale sur la cybercriminalité

Workshop on criminal legislation

Organised by the Ministry of Information and Communication Technology of Mauritius and the Council of Europe
Balaclava, Mauritius, 14 August 2014

Legal Frameworks in Mauritius: Reflections on Legislative Reform

Zahid Jamil
Council of Europe

www.coe.int/cybercrime

Funded by the European Union and the Council of Europe — EUROPEAN UNION

COUNCIL OF EUROPE — CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Reflections on Legislative Reform

Consideration:

- **Computer Misuse & Cybercrime Act 2003**
- **Information Communication Technology Act 2001**
- **Mutual Assistance in Criminal & Related Matters Act 2003**
- **Criminal Code**
- **The Unsolicited Commercial Electronic Messages Bill**

- **Amendments to Child Online Protection Bill**
- **Amendments to Data Protection Bill**

Reflections on Legislative Reform

Computer Misuse & Cybercrime Act 2003

Definitions:
Access
Unauthorized?
Technology specific [keys, digital signature, record… "tangible medium"]
Intercept [listening or recording]
Property [electronically produced]
Subscriber [user]
Underlying service [service used by computer system]
Modification [data interference (deterioration) vs. system interference (serious hindering)

Offences:
Unauthorized access & unauthorized access to **program or data**
Unlawful interception
E-forgery

3

Reflections on Legislative Reform

Computer Misuse & Cybercrime Act 2003

Powers:

Preservation - Judge
Interception – ICT Act – *"intercept' means intercept by listening or recording, by any means, a message passing over an information or communication network, including telecommunication network, without the knowledge of the person originating, sending or transmitting the message"*
Retention
Safeguards
Warrants
Right of Third Parties

Cross border cooperation

4

Reflections on Legislative Reform

Unauthorized Access

UK CMA	Mauritius CMACA
Access **of any kind** by any person to any **program or data** held in a computer is unauthorised if— (a)he is not himself entitled to control access of the kind in question **to the program or data**; and (b)he does not have consent to access by him of the kind in question **to the program or data** from any person who is so entitled but this subsection is subject to section 10.	(3) An access by a person to a computer system is unauthorised where the person – (a) is not himself entitled to control access of the kind in question; and (b) does not have consent to access by him of the kind in question from any person who is so entitled.

5

Reflections on Legislative Reform

Unlawful interception

Unauthorised access to and **interception** of computer service

(1) Subject to subsection (5), any person who, by any means, knowingly

(a) **secures access to any computer system** for the purpose of obtaining, directly or indirectly, any computer service;

(b) **intercepts or causes to be intercepted, directly or indirectly, any function of, or any data within a computer system**, shall commit an offence.

…….

(4) A person shall not be liable under subsection (1) where he –

(a) has the **express or implied consent** of **both the person who sent the data and the intended recipient** of such data;

(b) is acting in reliance of any statutory power.

6

Reflections on Legislative Reform

Unlawful interception

Unauthorised access to and **interception** of **[non-public transmission of computer data]** computer service

(1) Subject to subsection (5), any person who, by any means, knowingly

(a) **secures access to any computer system** for the purpose of obtaining, directly or indirectly, any computer service;

(b) **intercepts or causes to be intercepted, directly or indirectly, any function of, or any data within a computer system**, shall commit an offence.

…….

(4) A person shall not be liable under subsection (1) where he –

(a) has the **express or implied consent** of **both the person who sent the data and the intended recipient** of such data;

(b) is acting in reliance of any statutory power.

Reflections on Legislative Reform

7. Damaging or denying access to computer system

Any person who without lawful authority or lawful excuse, does an act which causes directly or indirectly –

(a) a degradation, failure, interruption or obstruction of the operation of a computer system; or

(b) a **denial of access** to, or impairment of **any program or data** stored in, the computer system, shall commit an offence and shall, on conviction be liable to a fine not exceeding 200,000 and to penal servitude not exceeding 20 years.

Reflections on Legislative Reform

8. Unauthorised disclosure of password

Any person who, knowingly discloses [FOR WHAT PURPOSE] any password, access code, or any other means of gaining access to any **program or data** held in any computer system –

(1) for any wrongful gain;
(2) for any unlawful purpose; or
(3) knowing that it is likely to cause prejudice to any person,
shall commit an offence and shall, on conviction, be liable to a fine not exceeding
50,000 rupees and to a term of imprisonment not exceeding 5 years.

Reflections on Legislative Reform

8. Unauthorised disclosure of password

Any person who, knowingly discloses [FOR WHAT PURPOSE] any password, access code, or any other means of gaining access to any **program or data** held in any computer system –

(1) for any wrongful gain;
(2) for any unlawful purpose; or
(3) knowing that it is likely to cause prejudice to any person,
shall commit an offence and shall, on conviction, be liable to a fine not exceeding
50,000 rupees and to a term of imprisonment not exceeding 5 years.

9. Unlawful possession of devices and data

(1) Any person who knowingly manufactures, sells, procures for use, imports, distributes or otherwise makes available, a computer system or any other device, designed or adapted **primarily for the purpose of committing any offence** under sections 3 to 8, shall commit an offence.

Reflections on Legislative Reform

E- Forgery

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, **the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data** with the **intent that it be considered or acted upon for legal purposes as if it were authentic**, regardless **whether or not the data is directly readable and intelligible**. A Party may require an **intent to defraud, or similar dishonest intent**, before criminal liability attaches.

Reflections on Legislative Reform

Section 105A. Electronic document or writing For the purposes of sections 106 to 109, 111 and 112, a document or writing includes any disc, tape, sound track or other device on or in which data is recorded or stored by mechanical, electronic or other means.
Section 108. Forgery by private individual of public or commercial writing Any other person who commits a forgery in an authenticated and public writing, or in a commercial or bank writing: (a) by **counterfeiting or altering any writing, date or signature, or by the use of a fictitious name**; (b) by **fabricating any agreement, condition, obligation or discharge, or inserting** it in any such act after it has been completed; or (c) by **adding to any clause, statement or fact which such act was intended to contain and certify, or by altering such clause, fact or statement**, shall be punished by penal servitude.
Section 111. Forgery of private writing Any person who, by one of the means specified in section 108, **forges a private writing**, shall be punished by penal servitude for a term not exceeding 20 years.

Reflections on Legislative Reform

ICT Act

– "intercept' means intercept by **listening or recording**, by any means, **a message passing** over an information or communication network, including telecommunication network, without the knowledge of the person originating, sending or transmitting the **message**"

(5) (a) Nothing in this Act shall prevent a public operator or any of his employees or agents from intercepting, withholding or otherwise dealing with a message which he has reason to believe is-
(i) indecent or abusive;
(ii) in contravention of this Act;
(iii) of a nature likely to endanger or compromise State's defence, or public safety or public order.

13

Reflections on Legislative Reform

(6) (a) **Nothing** in this Act shall **prevent a Judge in Chambers, upon an application, whether ex parte or otherwise, being made to him, by the Police**, from making an **order authorising a public operator, or any of its employees or agents, to intercept, withhold or disclose to the police, an information or communication message including a telecommunication message.**

(b) An order under paragraph (a) shall –

(i) not be made unless the Judge is satisfied that information relating to the message is **material to any criminal proceedings, whether pending or contemplated**, in Mauritius;
(ii) remain **valid for such period, not exceeding 60** days, as the Judge may determine;
(iii) **specify the place where the interception or withholding shall take place**.

Indemnity:
46 Any person who - (o) except as expressly permitted by this Act or as authorized by a Judge, intercepts, authorises or permits another person to intercept, or does any act or thing that will enable him or another person to intercept, a message passing over a network; shall commit an offence.

14

Reflections on Legislative Reform

Improvement in Language to CMACA powers

11. Preservation
- (Judge/time)

14. Powers of access, search and seizure
- (another computer - accessible and available to the initial system)
- (similarly secure)

Contd.

Reflections on Legislative Reform

Safeguards

- Criminal Code
- Warrants
- Grounds
- Limitations and scope (duration, time,
- Copies of data

Reflections on Legislative Reform

substantive grounds and reasons :

- explain why it is believed the material sought will be found on the premises to be searched;
- identify and explain with specificity the type of evidence suspected will be found on the premises;
- identify and explain with specificity the individual information system to be searched or seized;
- identify and explain with specificity the relevant program or data that is sought and reasonably suspected to be available from each individual information system;
- describe and identify the person(s) to be authorised to accompany the officer executing the warrant and the reasons that necessitate their presence;
- identify the Magistrate Frist Class who will be accompanying the officer during execution of the warrant;
- if authority to enter and search the premises on more than one occasion is needed, explain why, and how many, further entries are needed to achieve the purpose for which the warrant is to be issued;

Reflections on Legislative Reform

- what measures shall be taken to prepare and ensure that the search and seizure is carried out through technical means such as mirroring or copying of relevant data and not through physical custody of information systems or devices;
- why it is believed necessary to search premises occupied or controlled by the person in question;
- that it is not practicable to communicate with any person entitled to grant entry to the premises;
- why it is practicable to communicate with a person entitled to grant entry to the premises but it is not practicable to communicate with any person entitled to grant access to the evidence;
- why entry to the premises will not be granted unless a warrant is produced;
- why the purpose of a search may be frustrated or seriously prejudiced unless an investigating officer arriving at the premises can secure immediate entry to them; and
- why to achieve the purpose for which the warrant is being applied it is necessary that the warrant authorises entry to and search of each set of premises.

Reflections on Legislative Reform

Retention

Reflections on Legislative Reform

Mutual Assistance in Criminal & Related Matters Act 2003

Article 26 - Spontaneous information
Article 29 – Expedited preservation of stored computer data
Article 30 – Expedited disclosure of preserved traffic data
Article 31 – Mutual assistance regarding accessing of stored computer data
Article 32 – Trans-border access to stored computer data with consent or where publicly available
Article 33 – Mutual assistance regarding the real-time collection of traffic data
Article 34 – Mutual assistance regarding the interception of content data
Article 35 – 24/7 Network

CERT-MU

Reflections on Legislative Reform

The Unsolicited Commercial Electronic Messages Bill

Offence – Criminal Code: "offences which the law punishes as crimes, misdemeanours or contraventions"

CMACA : Powers to apply to all offences, crimes, investigations and prosecutions

Article 14 – Scope of procedural provisions

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b other criminal offences committed by means of a computer system; and

c the collection of evidence in electronic form of a criminal offence.

21

Reflections on Legislative Reform

US CAN-SPAM Act
Singapore Spam Control Act

The Bill:

Definitions:
Over defined, Defining restricts eg. "Account", "commercial activity"
"account" includes –
a free account;
a pre-paid account;
anything that may be reasonably regarded as the equivalent of an account;

"commercial activity" means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, whether or not the person who carries it out does so in the exception of profit, other than any transaction, act or conduct that is carried out for the purposes of service regulation by governmental or parastatal bodies, law enforcement, public safety, the protection of Mauritius, the conduct of international affairs or the defence of Mauritius.

22

Reflections on Legislative Reform

Sender of unsolicited commercial electronic messages in <u>bulk</u> to comply with Second Schedule **11.** Any person who sends, causes to be sent or authorises the sending of unsolicited commercial electronic messages in bulk shall comply with the requirements in the Second Schedule.	**5. Sending of an unsolicited commercial electronic message** (1) A person commits the offence of persistent sending of an unsolicited commercial electronic message when a second infringement is committed preceded by the commission of a first infringement.

Reflections on Legislative Reform

"unsolicited commercial electronic message" means a commercial electronic message which the recipient thereof has not given his consent to receiving;

"consented to receiving"-
(a) means express consent:
(i) that needs to be set out clearly and simply by the party seeking it,

(ii) whether given by the relevant electronic address-holder or any other person who uses the relevant electronic address; –

(b) means implied consent that can reasonably be inferred from the conduct and the business and other relationships of the persons concerned

Reflections on Legislative Reform

(c) means consent that is deemed to have been given when the following circumstances apply:

(i) an electronic address has been conspicuously published by a person in a business or official capacity and;

(ii) the publication of the address is not accompanied by a disclaimer to the effect that the relevant electronic address-holder does not want to receive unsolicited electronic address messages at that address and;

the message sent to that address is relevant to the business, role, functions, or duties of the person in a business or official capacity; but

(d) does not include the circumstances specified in the regulations from which consent cannot be inferred

25

Reflections on Legislative Reform

Unsolicited Commercial messages in bulk

Unsolicited Non-Commercial messages:

- Persistent / Protected Computer
- Dictionary Attacks
- Harvesting

26

Reflections on Legislative Reform

Thank you!

Zahid Jamil, Esq.
Barrister
zahid@jamilandjamil.com