ELECTRONIC CRIMES BILL

SAINT LUCIA

No. of 2009

AN ACT to provide for the prevention and punishment of electronic crimes and for related matters.

BE IT ENACTED by the Queen's Most Excellent Majesty by and with the advice of the House of Assembly and the Senate of Saint Lucia and the authority of the same as follows:

PART 1
PRELIMINARY

Short title and commencement

1. (1) This Act may be cited as the Electronic Crimes Act 2009.

(2) This Act shall come into force on a day to be fixed by the Minister by Order published in the *Gazette.*

Interpretation

2. In this Act -

"access" in the context of any electronic system means to communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of the electronic system;

"damage" includes modifying, altering, deleting, erasing, suppressing, changing location or making data temporarily unavailable, halting electronic system or chocking the networks;

"data " includes representations of facts, information or concepts that are being prepared or have been prepared in a form suitable for use in an electronic system including computer programme, text, images, sound, video and information within a database or electronic system;

"decryption" means the process of transforming or unscrambling encrypted data from its unreadable and incomprehensible format to its plain version;

"defamation" means defamation within the meaning of section 314 of the Criminal Code, Cap. 3.01;

"electronic" means relating to technology having electrical, digital, magnetic, optical, biometric, electrochemical, wireless, electromagnetic, or similar capabilities;

"electronic device" is any hardware that accomplishes its functions using any form or combination of electrical energy

"electronic system" means any electronic device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data and includes an electronic storage medium;

"encryption" means the process whereby data is transformed or scrambled from its plain version to an unreadable or incomprehensible format, regardless of the technique utilized for such transformation or scrambling and irrespective of the medium in which such data occurs or can be found for the purposes of protecting such data;

"function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within an electronic system;

"malicious code" means a computer program or a hidden function in a program that infects data with or without attaching its copy to a file and is capable of spreading over electronic system with or without human intervention including virus, worm or Trojan horse.

"minor" means a person below the age of eighteen years;

"plain version" means original data before it has been transformed or scrambled to an unreadable or incomprehensible format;

"service provider" means—

(a) a person who provides an information and communication service including the sending, receiving, storing or processing of the electronic communication or the provision of other services in relation to it through any electronic system;

(b) a person who owns, possesses, operates, manages or controls a public switched network or provides telecommunication services; or

(c) any other person that processes or stores data on behalf of such electronic communication service or users of such service;

"subscriber" means a person using the services of a service provider;

"subscriber information" means any information contained in any form that is held by a

service provider, relating to subscribers of its services other than traffic data and by which can be established-

(a) the type of communication service used, the technical provisions taken thereto and the period of service;

(b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; or

(c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement;

"traffic data" means any data relating to a communication by means of an electronic system, generated by an electronic system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service; and

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

Application

3. This Act applies where-

(a) an offence under this Act was committed in Saint Lucia;

(b) any act of preparation towards an offence under this Act or any part of the offence was committed in Saint Lucia, or where any result of the offence has had an effect in Saint Lucia;

(c) an offence under this Act was committed by a Saint Lucian national or a person resident or carrying out business in Saint Lucia or visiting Saint Lucia or staying in transit in Saint Lucia;

(d) an offence under this Act was committed in relation to or connected with an electronic system or data in Saint Lucia or capable of being connected, sent to, used by or with any electronic system in Saint Lucia; or

(e) an offence under this Act was committed by any person, of any nationality or citizenship or in any place outside or inside Saint Lucia, having an effect on the security of Saint Lucia or its nationals, or having universal application under international law, custom and usage.

Binding on Crown

4. This Act binds the Crown.

PART 2

OFFENCES

Criminal access

5. (1) A person shall not gain unauthorized access to the whole or any part of an electronic system with or without infringing security measures, with intent to infringe privacy or commit a further offence.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years, or to both.

Criminal data access

6. (1) A person shall not cause an electronic system to perform any function for the purpose of gaining access to any data held in an electronic system knowing that the access he or she intends to secure is unauthorized.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years or to both.

Cyber stalking

7. (1) A person shall not intimidate, coerce, insult or annoy another person using an electronic system.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years or to both.

Cyber terrorism

8. (1) A person shall not, in furtherance of any criminal, political or social objective, commit a premeditated attack against an electronic system or data, which results in the injury or death of any person or causes extreme financial harm to that person.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years or to both.

Data damage

9. (1) A person shall not with intent to cause damage to the public or any person, damage any data.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years, or to both.

For the purpose of this section "damage" includes the unauthorized modification of data held in an electronic system.

Electronic defamation

10. (1) A person shall not defame another person using an electronic system.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years or to both.

Electronic forgery

11. (1) A person shall not, interfere with data or an electronic system with the intention that he, she, or another person uses the data or the electronic system to induce somebody to accept it as genuine and by reason of so accepting it to do or not to do any act to his or her own or any other person's prejudice or injury.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years or to both.

Electronic fraud

12. (1) A person shall not for gain, interfere with data or an electronic system-

(a) to induce any person to enter into a relationship; or

(b) with intent to deceive any person.

which act is likely to cause damage or harm to that person or any other person.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years or to both.

Malicious code

13. (1) A person shall not write, offer, make available, distribute or transmit a malicious code through an electronic system.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years or to both.

Misuse of devices

14. (1) A person shall not produce, possess, sell, procure, import, distribute or otherwise make available-

(a) a device, including a computer program designed or adapted primarily for
(b) a password, access code, or similar data by which the whole or any part of an electronic system is capable of being accessed with the intent that it be used for the purpose of committing an offence under this Act.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years or to both.

(3) This section does not apply where the production, possession, sale, procurement, import, distribution or otherwise making available of a device is not primarily for the purpose of committing an offence under this Act but is a lawful purpose including the authorized testing or protection of an electronic system.

Misuse of encryption

15. (1) A person shall not for the purpose of commission of an offence or concealment of incriminating evidence, knowingly and willfully encrypt any incriminating communication or data contained in an electronic system relating to the offence or incriminating evidence.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years or to both.

Pornography

16. (1) A person shall not, intentionally, through or in an electronic system -

(a) produce pornographic material for the purpose of its distribution;
(b) offer or make pornographic material available; distribute or transmit pornography;
(c) procure pornographic material for his or herself or for another person; or
(d) retain pornographic material.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years or to both.

(3) Notwithstanding subsections (1) and (2), where the pornographic material referred to in subsection (1) –

(a) a minor or a person appearing to be a minor, engaged in sexually explicit conduct; or

(b) images representing a minor engaged in sexually explicit conduct picture of a minor,

the person commits an offence of child pornography and is liable on conviction to a fine not exceeding five hundred thousand dollars or to imprisonment for a term not exceeding three years or to both.

(4) It is a defence to an offence under subsection (1) or (2) that pornographic material is produced, offered, distributed procured for bona fide research or medical purposes.

Sensitive electronic system

17. (1) A person shall not knowingly or willfully disable or obtain access to a sensitive electronic system whether or not in the course of commission of another offence under this Act.

(2) A person who contravenes subsection (2) commits an offence and is liable on conviction to a fine not exceeding three hundred thousand dollars or to imprisonment for a term not exceeding ten years or to both.

(3) For the purposes of this section-

"sensitive electronic system" is an electronic system used directly in connection with or necessary for —

(a) the security, defence or international relations of Saint Lucia;

(b) the existence or identity of a confidential source of information relating to the enforcement of criminal law;

(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, courts, public transportation or public key infrastructure;

(d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services ; or

(e) the purpose declared as such by the Minister by Order published in the *Gazette*.

Spamming

18. (1) A person shall not transmit an unsolicited electronic message to any person or electronic system to show an unsolicited message, without the express permission of the recipient.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years or to both.

Spoofing

19. (1) A person shall not establish a website or send an electronic message with a counterfeit source-

(a) with the intention that the recipient or visitor or an electronic system will believe it to be an authentic source; or

(b) to attract or solicit any person or electronic system;

for the purpose of gaining unauthorized access to commit a further offence or obtain information which can be used for unlawful purposes.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years or to both.

System damage

20. (1) A person shall not, with intent to cause damage to the public or any person, interfere with, interrupt or obstruct the functioning, reliability or usefulness of an electronic system by inputting, transmitting, damaging or deteriorating any data.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years, or to both.

Unauthorized access to code

21. (1) A person shall not disclose or obtain any password, access code or any other means of gaining access to any electronic system or data with intent to obtain wrongful gain or inflict wrongful loss to any person or for any unlawful purpose.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years or to both.

Unauthorized interception

22. (1) A person shall not, without lawful authority intercept by technical means, non- public transmissions of data to, from or within an electronic system.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years or to both.

PART 3
INVESTIGATIONS AND PROCEDURES

Preservation order

23. (1) A police officer may apply to a Judge in Chambers for an order for the expeditious preservation of data that has been stored or processed by means of an electronic system, where there are reasonable grounds to believe that the data is vulnerable to loss or modification and where such data is required for the purposes of a criminal investigation or the prosecution of an offence.

(2) For the purposes of subsection (1), data includes traffic data and subscriber information.

(3) An order made under subsection (1) remains in force-

(a) until such time as may be reasonably be required for the investigation of an offence;

(b) where prosecution is instituted, until the final determination of the case; or

(c) until such time as the judge in Chambers determines necessary.

Disclosure of preserved data

24. A police officer may, for the purposes of a criminal investigation or the prosecution of an offence, apply to a Judge in Chambers for an order for the disclosure of-

(a) any preserved data, irrespective of whether one or more service provides were involved in the transmission of the data;

(b) sufficient data to identify the service providers and the path through which the data was transmitted; or

(c) the electronic key enabling access to or the interpretation of data.

Production order

25.(1) If the disclosure of data is required for the purpose of a criminal investigation or the prosecution of an offence, a police officer may apply to a Judge in Chambers for an order compelling-

(a) a person to submit specified data in that person's possession or control, which is stored in a computer system;
(b) a service provider offering its services to submit subscriber information in relation to the services in that service provider's possession and control.

(2) Where any material to which an investigation relates consists of data stored in an electronic system, disc, cassette, or on microfilm, or preserved by any mechanical or electronic device, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

Powers of access, search and seizure for the purpose of investigation

26. (1) Where a police officer has reason to believe that stored data would be relevant for the purposes of an investigation or the prosecution of an offence, the police officer may apply to a Judge in Chambers for the issue of a warrant to enter any premises to access, search and seize that data.

(2) In the execution of a warrant under subsection (1), the powers of the police officer shall include the power to-

(a) access, inspect and check the operation of any computer system;
(b) use or cause to be used any computer system to search any data contained in or available to the computer system;
(c) access any information, code or technology which has the capability of transforming or unscrambling encrypted data contained or available to an electronic system into readable and comprehensible format or text for the purpose of investigating any offence under this Act or any other offence which is disclosed in the course of the lawful exercise of the powers under this section;
(d) require any person in possession of the decryption information to grant the police officer access to such decryption information necessary to decrypt data required for required for the purpose of investigating the offence.
(e) seize or secure an electronic system.

(3) A person shall not-

(a) obstruct a police officer in the exercise of the police officer's powers under this section; or
(b) fail to comply with a request made by a police officer under this section.

(4) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding one year, or both.

For the purposes of this section-

"decryption information" means information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable and incomprehensible format to its plain text version;

"encrypted data" means data which has been transformed or scrambled from its plain text version to an unreadable and incomprehensible format, regardless of the technique utilized for transformation or scrambling, and irrespective of the medium in which such data occurs or can be found for the purposes of protecting the content of such data;

"plain text version" means original data before it has been transformed or scrambled to an unreadable or incomprehensible format.

Real time collection of traffic data

27. Where a police officer has reasonable grounds to believe that any data would be relevant for the purposes of investigation and prosecution of an offence under this Act, the police officer may apply to a Judge in Chambers for an order-

(a) allowing the collection or recording of traffic data, in real time, associated with specified communications transmitted by means of any computer system; or
(b) compelling a service provider, within its technical capabilities, to-
effect such collection and recording referred to in paragraph (a), or
assist the police officer, to effect such collection and recording.

Arrest without warrant

28. A police officer may, without warrant, arrest any person reasonably suspected of committing an offence under this Act.

Deletion

29. A Judge in Chambers may, on application by a police officer and being satisfied that an electronic system contains data that is indecent photographs of children, order that the data be-

(a) no longer stored on or be made available through the electronic system; or
(b) deleted or destroyed.

Limited use of data and information

30. A person shall not use or disclose data obtained pursuant to this Part for any purpose other than that for which the data was originally sought except-

(a) in accordance with any other enactment;
(b) in compliance with an order of the Judge or;
(c) where the data is required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, assessing or collecting tax, duty or other monies owed or payable the Government;
(d) for the prevention of injury or other damage to the health of a person or serious loss or damage to property; or
(e) in the public interest.

PART 4
MISCELLANEOUS

Institution of criminal proceedings

31. Criminal proceedings shall not be instituted under this Act except on an information filed by, or with the consent of, the Director of Public Prosecutions.

Extraditable offences

32. An offence pursuant to Part 2 shall be considered to be extraditable crimes for which extradition may be granted or obtained under the Extradition Act, Cap 2.10.

Order for compensation

33. (1) A court before which a person is convicted of an offence under this Act may make an order against that person for the payment by that person of sum of money fixed by the Court by way of compensation to any person for any damage caused to his or her computer system, program or data by the offence in respect of which the sentence is passed.

(2) A claim by a person for damages sustained by reason of the offence shall be deemed to have been satisfied to the extent of any amount which has been paid to him or her under an order for compensation, except that the order shall not prejudice any right to a civil remedy for the recovery of damages beyond the amount of compensation paid under the order.

(3) An order for compensation under this section shall be recoverable as a civil debt.

Forfeiture

34. (1) The Court before which a person is convicted of an offence under this Act may, in addition to this any penalty imposed , order the forfeiture of any apparatus, article or thing which

is the subject matter of the offence or is used in the connection with the commission of the offence.

(2) In addition to making an order that obscene matter forming part of the subject matter of the offence is forfeited, the Court shall, where appropriate, order that the obscene matter be deleted from or no longer stored or made available through the electronic system.

Regulations

35. The Minister may make Regulations for the purposes of giving effect to the provisions of this Act.