SAINT VINCENT AND THE GRENADINES

CYBERCRIME BILL 2016

ARRANGEMENT OF SECTIONS

SECTION

PART I

PRELIMINARY

1. Short title and commencement
2. Interpretation

PART II

OFFENCES

3. Illegal access to computer system
4. Illegal remaining in computer system
5. Illegal interception
6. Illegal data interference
7. Illegal acquisition of data
8. Illegal system interference
9. Offences affecting critical infrastructure
10. Illegal devices
11. Identity-related crimes
12. Computer-related forgery
13. Computer-related fraud
14. Violation of privacy
15. Child pornography
16. Harassment utilizing means of electronic communication
17. Spam
18. Spoofing

PART III

INVESTIGATIONS AND PROCEDURES

19. Expedited preservation
20. Disclosure of traffic data
21. Production order
22. Collection of traffic data
23. Interception of content data

24. Order for removal or disablement of data
25. Limited use of data and information
26. Disclosure of details of notice or order
27. Remote forensic tools
28. Order for payment of compensation
29. Forfeiture
30. Order for seizure and restraint
31. Jurisdiction
32. Offence by body corporate
33. Search and seizure
34. Assistance
35. Institution of criminal proceedings
36. Arrest with warrant
37. Extraditable offences

PART IV

LIABILITY OF INTERNET SERVICE PROVIDERS

38. No monitoring obligation
39. Access provider
40. Hosting provider
41. Caching provider
42. Hperlinks provider
43. Search engine provider

PART V

MISCELLANEOUS

44. Regulations

SCHEDULE

SAINT VINCENT AND THE GRENADINES

BILL FOR

_____

ACT NO. OF 2016

I ASSENT

Governor - General

[ ]

AN ACT to provide for the creation of offences related to cybercrimes and for related matters.

[ ]

BE IT ENACTED by the Queen's Most Excellent Majesty, by and with the advice and consent of the House of Assembly of Saint Vincent and the Grenadines and by the authority of the same, as follows:

PART I

PRELIMINARY

Short title and commencement

1. (1) This Act may be cited as the Cybercrime Act, 2016.

(2) This Act comes into force on a day to be appointed by the Governor-General by Proclamation published in the *Gazette*.

Interpretation

2. In this Act –

"apparatus" includes –

(a) a computer system or part of a computer system; or

(b) a computer data storage medium;

"child" means a person under the age of eighteen years;

"child pornography" means material that –

(a) depicts or presents a child engaged in sexual activity or conduct;

(b) depicts or presents a child in a sexually explicit pose;

(c) depicts or presents, for sexual purposes, parts of a child's body pasted to visual representations of parts of an adult's body or vice versa;

(d) depicts or presents, for sexual purposes, parts of a child's body which have been rendered complete by computer generated images or by other methods of visual representation;

(e) depicts or presents a person appearing to be a child engaged in sexual conduct; or

(f) realistically represents a person appearing to be a child engaged in sexual conduct,

and includes, but is not limited to, any visual material including images, animations or videos, or audio or text material, but does not include any visual representation produced or reproduced for the purpose of education, counseling, or promotion of reproductive health or as part of a criminal investigation or prosecution or civil proceedings or in the lawful performance of a person's profession, duties and functions;

"computer data" means any representation of –

(a) facts;

(b) concepts;

(c) information including text, sound, image or video; or

(d) machine-readable code or instructions,

that is in a form suitable for processing in a computer system and is capable of being sent, received or stored, and includes a program that can cause a computer system to perform a function;

"computer data storage medium" means anything in which information is capable of being stored, or anything from which information is capable of being retrieved or reproduced, with or without the aid of any other article or device;

"computer program" or "program" means data which represents instructions or statements that, when executed in a computer system, can cause the computer system to perform a function;

"computer system" means a device or a group of inter-connected or related devices which follows a program or external instruction to perform automatic processing of information or electronic data;

"device" includes –

(a) a component of a computer system such as a graphic card or memory chip;

(b) a storage component such as a hard drive, memory card, compact disc or tape;

(c) input equipment such as a keyboard, mouse, track pad, scanner or digital camera; or

(d) output equipment such as a printer or screen;

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

"function" in relation to a computer system includes logic, control, arithmetic, deletion, storage or retrieval and communication or telecommunication to, from or within a computer;

"hinder" in relation to a computer system includes –

(a) disconnecting the electricity supply to a computer system;

(b) causing electromagnetic interference to a computer system;

(c) corrupting a computer system; and

(d) inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data;

"intercept" in relation to computer data communication includes listening to, monitoring, viewing, reading or recording, by any means, such communication during transmission without the knowledge of the person making or receiving the communication;

"internet service provider" includes a person who provides the services mentioned in sections 38 to 43;

"Minister" means the Minister to whom responsibility for legal affairs is assigned;

"multiple electronic mail messages" means any unsolicited electronic message, including electronic mail and instant message, that is sent to more than a thousand recipients at a time;

"remote forensic tools" means investigative software or hardware installed on or attached to a computer system that is used to perform a task that includes keystroke logging or transmission of an internet protocol address;

"traffic data" means computer data that –

(a) relates to a communication by means of a computer system;

(b) is generated by a computer system that is part of the chain of communication; and

(c) shows the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

PART II

OFFENCES

Illegal access to computer system

3. A person who, intentionally and without lawful excuse or justification, accesses a computer system or any part of a computer system commits an offence and is liable on –

(a) summary conviction to a fine of two hundred thousand dollars or to imprisonment for three years or to both;

(b) conviction on indictment to a fine of five hundred thousand dollars or to imprisonment for seven years or to both.

Illegal remaining in computer system

4. (1) A person who, intentionally and without lawful excuse or justification, remains logged into a computer system or part of a computer system or continues to use a computer system, commits an offence and is liable on –

(a) summary conviction to a fine of two hundred thousand dollars or to imprisonment for three years or to both;

(b) conviction on indictment to a fine of five hundred thousand dollars or to imprisonment for seven years or to both.

Illegal interception

5. (1) A person who, intentionally and without lawful excuse or justification, intercepts –

(a) any subscriber information or traffic data or any communication to, from or within a computer system; or

(b) any electromagnetic emission from a computer system,

commits an offence.

(2) A person who commits an offence under subsection (1) is liable on –

(a) summary conviction to a fine of two hundred thousand dollars or to imprisonment for three years or to both;

(b) conviction on indictment to a fine of five hundred thousand dollars or to imprisonment for seven years or to both.

Illegal data interference

6. (1) A person who, intentionally and without lawful excuse or justification –

(a) damages computer data or causes computer data to deteriorate;

(b) deletes computer data;

(c) alters computer data;

(d) renders computer data meaningless, useless or ineffective;

(e) obstructs, interrupts or interferes with the lawful use of computer data;

(f) obstructs, interrupts or interferes with a person in the lawful use of computer data; or

(g) denies access to computer data to a person authorized to access it,

commits an offence.

(2) A person who commits an offence under subsection (1) is liable on –

(a) summary conviction to a fine of two hundred thousand dollars or to imprisonment for three years or to both;

(b) conviction on indictment to a fine of five hundred thousand dollars or to imprisonment for seven years or to both.

Illegal acquisition of data

7. A person who, intentionally and without lawful excuse or justification, obtains for himself or for another person, computer data which is not meant for him or the other person and which is protected against unauthorized access, commits an offence and is liable on –

(a) summary conviction to a fine of two hundred thousand dollars or to imprisonment for three years or to both;

(b) conviction on indictment to a fine of five hundred thousand dollars or to imprisonment for seven years or to both.

Illegal system interference

8. (1) A person who, intentionally and without lawful excuse or justification –

(a) hinders or interferes with the functioning of a computer system; or

(b) hinders or interferes with a person who is lawfully using or operating a computer system,

commits an offence.

(2) A person who commits an offence under subsection (1) is liable on –

(a) summary conviction to a fine of two hundred thousand dollars or to imprisonment for three years or to both;

(b) conviction on indictment to a fine of five hundred thousand dollars or to imprisonment for seven years or to both.

Offences affecting critical infrastructure

9. (1) Notwithstanding the penalties set out in sections 3 to 8, where a person commits an offence under any of those sections and the offence results in hindering or interference with a computer system that –

(a) is exclusively for the use of critical infrastructure; or

(b) affects the use, or impacts the operation, of critical infrastructure,

the person is liable on conviction on indictment to a fine of one million dollars or to imprisonment for fifteen years.

(2) For the purposes of this section, “critical infrastructure” means any computer system, device, network, computer program, computer data, so vital to Saint Vincent and the Grenadines that the incapacity or destruction of,

or interference with, such system, device, network, computer program or computer data would have a debilitating impact on –

(a) security, defence or international relations of Saint Vincent and the Grenadines; or

(b) provision of services directly related to national or economic security, banking and financial services, public utilities, the energy sector, communications infrastructure, public transportation, public health and safety, or public key infrastructure.

Illegal devices

10. (1) A person who produces, sells, procures for use, imports, exports, distributes or otherwise makes available or has in his possession –

(a) a device, including a computer program, that is designed or adapted for the purpose of committing an offence under this Act; or

(b) a computer password, access code or similar data by which the whole or any part of a computer system, computer data storage medium or computer data is capable of being accessed,

with the intent that it be used for the purpose of committing an offence under this Act commits an offence.

(2) A person who commits an offence under subsection (1) is liable on –

(a) summary conviction to a fine of two hundred thousand dollars or to imprisonment for three years or to both;

(b) conviction on indictment to a fine of five hundred thousand dollars or to imprisonment for seven years or to both.

Identity-related crimes

11. (1) A person who, intentionally and without lawful excuse or justification transfers, possesses or uses a means of identification, other than his own, with the intent of committing, or aiding or abetting, the commission of, an unlawful act through the use of a computer system commits an offence.

(2) A person who commits an offence under subsection (1) is liable on –

(a) summary conviction to a fine of two hundred thousand dollars or to imprisonment for three years or to both;

(b) conviction on indictment to a fine of five hundred thousand dollars or to imprisonment for seven years or to both.

Computer-related forgery

12. (1) A person who, intentionally and without lawful excuse or justification inputs, alters, deletes, or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the computer data is directly readable and intelligible commits an offence.

(2) A person who commits an offence under subsection (1) is liable on –

(a) summary conviction to a fine of two hundred thousand dollars or to imprisonment for three years or to both;

(b) conviction on indictment to a fine of five hundred thousand dollars or to imprisonment for seven years or to both.

(3) A person who commits an offence under subsection (1) by sending out multiple electronic mail messages from or through a computer system is liable on conviction to a fine of ten thousand dollars and imprisonment for three years in addition to the penalty set out in subsection (2).

Computer-related fraud

13. (1) A person who, intentionally and without lawful excuse or justification–

(a) inputs, alters, deletes or suppresses computer data; or

(b) interferes with the functioning of a computer system,

with the fraudulent or dishonest intent of procuring an economic benefit for himself or another person and thereby causes a loss of, or damage to, property commits an offence.

(2) A person who commits an offence under subsection (1) is liable on –

(a) summary conviction to a fine of two hundred thousand dollars or to imprisonment for three years or to both;

(b) conviction on indictment to a fine of five hundred thousand dollars or to imprisonment for seven years or to both.

Violation of privacy

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

(a) captures;

(b) stores in, or publishes or transmits through a computer system,

the image of a private area of another person without his consent where the other person has a reasonable expectation that –

(i) he could disrobe in privacy; or

(ii) his private area would not be visible to the public, regardless of whether he is in a public or private place,

commits an offence.

(2) A person who commits an offence under subsection (1) is liable on–

(a) summary conviction to a fine of one hundred thousand dollars or to imprisonment for two years or to both;

(b) conviction on indictment to a fine of two hundred and fifty thousand dollars or to imprisonment for five years or to both.

(3) For the purposes of this section –

"capture" in relation to an image, means to videotape, photograph, film or record by any means;

"private area" means the genitals, pubic area, buttocks or breast;

Child pornography

15. (1) A person who, intentionally –

(a) produces child pornography for the purpose of its distribution through a computer system;

(b) offers to make available child pornography through a computer system;

(c) distributes or transmits child pornography through a computer system;

(d) procures or obtains child pornography through a computer system for himself or another person;

(e) possesses child pornography in a computer system or on a computer data storage medium; or

(f) obtains access to child pornography through information and communication technologies,

commits an offence.

(2) A person who commits an offence under subsection (1) is liable on –

(a) summary conviction to a fine of three hundred thousand dollars or to imprisonment for three years or to both;

(b) conviction on indictment to a fine of five hundred thousand dollars or to imprisonment for twenty years or to both.

Harassment utilizing means of electronic communication

16. (1) A person who uses a computer system to cyberbully, intentionally or recklessly, another person commits an offence.

(2) A person who uses a computer system to disseminate any information, statement or image, knowing the same to be false, and who –

(a) damages the reputation of another person; or

(b) subjects another person to public ridicule, contempt, hatred or embarrassment,

commits an offence.

(3) A person who, intentionally or recklessly –

(a) uses a computer system to disseminate any information, statement or image; and

(b) exposes the private affairs of another person, thereby subjecting that other person to public ridicule, contempt, hatred or embarrassment,

commits an offence.

(4) A person who commits an offence under this section is liable on –

(a) summary conviction to a fine of one hundred thousand dollars or to imprisonment for two years or to both;

(b) conviction on indictment to a fine of two hundred thousand dollars or to imprisonment for five years or to both.

(5) For the purpose of this section, "cyberbully" means to use a computer system repeatedly or continuously to convey information which causes –

(a) fear, intimidation, humiliation, distress or other harm to another person; or

(b) detriment to another person's health, emotional well-being, self-esteem or reputation.

Spam

17. (1) A person who, intentionally and without lawful excuse or justification –

(a) initiates the transmission of multiple electronic mail messages from or through a computer system; or

(b) uses a computer system to relay or retransmit multiple electronic mail messages, with the intent to deceive or mislead a user or internet service provider as to the origin of such messages,

and thereby causes harm to a person or damage to a computer system commits an offence.

(2) A person who intentionally falsifies the header information of an electronic mail message for the purpose of committing an offence under subsection (1) commits an offence.

(3) A person who commits an offence under this section is liable on –

(a) summary conviction to a fine of one hundred thousand dollars or to imprisonment for two years or to both;

(b) conviction on indictment to a fine of two hundred thousand dollars or to imprisonment for five years or to both.

Spoofing

18. (1) A person who establishes a website or sends an electronic mail message with a counterfeit source –

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

(b) to attract or solicit a person or computer system,

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

(2) A person who commits an offence under subsection (1) is liable on –

(a) summary conviction to a fine of one hundred thousand dollars or to imprisonment for two years or to both;

(b) conviction on indictment to a fine of two hundred thousand dollars or to imprisonment for five years or to both.

PART III

INVESTIGATIONS AND PROCEDURES

Expedited preservation

19. (1) A Judge may, if satisfied on an *ex parte* application by a police officer that there is reasonable ground to believe that computer data that is reasonably required for the purpose of a criminal investigation or criminal proceedings is vulnerable to loss or modification, authorise the police officer to require a person in control of the computer data, by notice in writing, to preserve the data for a period not exceeding ninety days as is specified in the notice.

(2) A Judge may, on *ex parte* application by a police officer, authorise an extension of the period referred to in subsection (1) by a further period not exceeding ninety days.

Disclosure of traffic data

20. A Judge may, if satisfied on an *ex parte* application by a police officer that there is reasonable ground to believe that computer data stored in a computer system is reasonably required for the purpose of a criminal investigation or criminal proceedings, require a person to disclose sufficient traffic data about a specified communication to identify –

(a) the internet service provider; or

(b) the path,

through which the communication was transmitted.

Production order

21. A Judge may, if satisfied on an *ex parte* application by a police officer that computer data, a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, order –

(a) a person in Saint Vincent and the Grenadines in control of a computer system, to produce from the computer system specified computer data or a printout or other intelligible output of the computer data; or

(b) an internet service provider in Saint Vincent and the Grenadines, to produce information about a person who subscribes to or otherwise uses its service.

Collection of traffic data

22. (1) A Judge, if satisfied on an *ex parte* application by a police officer that there is reasonable ground to believe that traffic data associated with a specified communication is reasonably required for the purpose of a criminal investigation or criminal proceedings, may order a person in control of the traffic data to –

(a) collect or record traffic data associated with a specified communication during a specified period; or

(b) permit and assist a specified police officer to collect or record that data.

(2) A Judge, if satisfied on an *ex parte* application by a police officer that there is reasonable ground to believe that traffic data is reasonably required for the purpose of a criminal investigation, may authorize a police officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means.

Interception of content data

23. A Judge, if satisfied on an *ex parte* application by a police officer that there is reasonable ground to believe that the content of electronic communications is reasonably required for the purpose of a criminal investigation or criminal proceedings, may –

(a) order an internet service provider in Saint Vincent and the Grenadines through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or

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

Order for removal or disablement of data

24. If a Judge is satisfied, on an *ex parte* application by a police officer, that an internet service provider or any other entity with a domain name server is storing, transmitting or providing access to computer data in contravention of this Act or any other written law, the Judge may order the internet service provider or other entity with a domain name server, to remove, or disable access to, the computer data.

Limited use of data and information

25. A person who uses or discloses data obtained under this Part for any purpose other than that for which the data was originally sought except –

(a) in accordance with any other written law;

(b) in compliance with an order of a Judge;

(c) where the data is required for the purpose of preventing, detecting or investigating offences or apprehending or prosecuting offenders;

(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,

commits an offence and is liable, on conviction, to a fine of one hundred thousand dollars or to imprisonment for two years or to both.

Disclosure of details of notice or order

26. If a notice under section 19 or an order under section 21 stipulates that confidentiality is to be maintained or an obligation of confidentiality is required to be maintained by law, a person who is the subject of the notice or order and who intentionally and without lawful excuse or justification discloses –

(a) the fact that the notice or order has been made;

(b) the details of the notice or order;

(c) anything done under the notice or order; or

(d) any data collected or recorded under the notice or order;

commits an offence and is liable, on conviction, to a fine of one hundred thousand dollars or to imprisonment for two years or to both.

Remote forensic tools;

Schedule

27. (1) If a Judge is satisfied on *ex parte* application by a police officer, that there is reasonable ground to believe that computer data which is required for the purpose of a criminal investigation into an offence listed in the Schedule, cannot be collected without the use of a remote forensic tool, the Judge may authorise a police officer, with such assistance as may be necessary, to utilize a remote forensic tool for the investigation.

(2) An application under subsection (1) shall contain the following information –

(a) the name and if possible, the address, of the person who is believed of committing the offence;

(b) a description of the targeted computer system;

(c) a description of the required tool, and the extent and duration of its utilization; and

(d) reason for the use of the tool.

(3) Where an application is made under subsection (1), the Judge may order that an internet service provider support the installation of the remote forensic tool.

(4) Where a remote forensic tool is utilized under this section –

(a) modifications to a computer system shall be limited to those that are necessary for the investigation;

(b) modifications to a computer system shall be undone, so far as possible, after the investigation; and

(c) the following information shall be logged –

(i) the technical means used;

(ii) the time and date of the application;

(iii) the identification of the computer system and details of the modification undertaken; and

(iv) the information obtained.

(5) The police officer responsible for a criminal investigation in which a remote forensic tool is utilized under this section shall ensure that any information obtained by the utilization of the remote forensic tool is protected against modification, unauthorized deletion and unauthorized access.

(6) An authorization that is granted under this section shall cease to apply where –

(a) the computer data sought is collected;

(b) there is no longer any reasonable ground for believing that the computer data sought exists; or

(c) the conditions of the authorization are no longer present.

(7) The Minister may, by order published in the *Gazette*, amend the Schedule.

(8) For the purpose of this section, “utilize” includes –

(a) accessing a computer system;

(b) developing a remote forensic tool;

(c) adopting a remote forensic tool; or

(d) acquiring a remote forensic tool.

Order for payment of compensation

28. (1) Where a person is convicted of an offence under this Act and the court before which the person is convicted is satisfied that another person has suffered loss or damage because of the commission of the offence, the court, may in addition to any penalty imposed under this Act, order the person convicted to pay a fixed sum as compensation to that other person for the loss or damage caused or likely to be caused as a result of the commission of the offence.

(2) An order made under subsection (1) shall be without prejudice to any other remedy which the person who suffered the loss or damage may have under any other law.

(3) The court may make an order under this section of its own motion or upon application of a person who has suffered the loss or damage as a result of the commission of the offence.

(4) A person who makes an application under subsection (3) shall do so before sentence is passed on the person against whom the order is sought.

(5) For the purposes of this section, computer data held in an apparatus is deemed to be the property of the owner of the apparatus.

Forfeiture

29. (1) Subject to subsection (2), where a person is convicted of an offence under this Act, the court before which the person is convicted may order that any property –

(a) used for or in connection with; or

(b) obtained as a result of or in connection with,

the commission of the offence, be forfeited to the Crown.

(2) Before making an order under subsection (1), the court shall give an opportunity to be heard to any person who claims to be the owner of the property or who appears to the court to have an interest in the property.

(3) Property forfeited to the Crown under this section shall vest in the Crown –

(a) if no appeal is made against the order, at the end of the period within which an appeal may be made against the order; or

(b) if an appeal has been made against the order, on the final determination of the matter, where the decision is made in favour of the Crown.

(4) Where property is forfeited to the Crown under this section, it shall be disposed of in the prescribed manner.

Order for seizure and restraint

30. Where an *ex parte* application is made by the Director of Public Prosecutions to a Judge and the Judge is satisfied that there is reasonable ground to believe that there is in any building, place or vessel, any property in respect of which a forfeiture order under section 31 has been made, the Judge may issue –

(a) a warrant authorizing a police officer to search the building, place or vessel for that property and to seize that property if found, and any other property in respect of which the police officer believes, on reasonable grounds, that a forfeiture order under section 31 may be made; or

(b) a restraint order prohibiting any person from disposing of, or otherwise dealing with any interest in, the property, other than as may be specified in the restraint order.

Jurisdiction

31. (1) A court in Saint Vincent and the Grenadines has jurisdiction in respect of an offence under this Act where the act constituting the offence is carried out –

(a) wholly or partly in Saint Vincent and the Grenadines;

(b) wholly or partly on board a vessel or aircraft registered in Saint Vincent and the Grenadines;

(c) wholly or partly outside Saint Vincent and the Grenadines, by a citizen of Saint Vincent and the Grenadines or body corporate incorporated under the laws of Saint Vincent and the Grenadines; or

(d) wholly or partly outside Saint Vincent and the Grenadines, by a person other than a citizen if the person's conduct would also constitute an offence under a law of the country where the offence was committed.

(2) For the purposes of subsection (1) (a), an act is carried out in Saint Vincent and the Grenadines if –

(a) the person is in Saint Vincent and the Grenadines at the time the act is committed;

(b) a computer system located in Saint Vincent and the Grenadines or computer data on a computer data storage medium located in Saint Vincent and the Grenadines is affected by the act; or

(c) the effect of the act, or the damage resulting from the act, occurs within Saint Vincent and the Grenadines.

Offence by body corporate

32. Where a body corporate commits an offence under this Act and a court is satisfied that a director, manager, secretary or other similar officer of the body corporate or, or any person who purports to act in such capacity –

(a) connived in or consented to the commission of the offence; or

(b) failed to exercise due diligence to prevent the commission of the offence,

the director, manager, secretary or other similar officer or person purporting to act in that capacity also commits the offence.

Search and seizure

33. (1) A Judge, if satisfied on the basis of an affidavit that there is reasonable ground to believe that there is in a place an apparatus or computer data –

(a) that may be material as evidence in proving an offence under this Act; or

(b) that has been acquired by a person as a result of an offence under this Act;

may issue a warrant authorizing a police officer, with such assistance as may be necessary, to enter the place to search for and seize the apparatus or computer data.

(2) If the police officer who is undertaking a search under this section has reasonable grounds to believe that –

(a) the computer data sought is stored in another computer system; or

(b) part of the computer data sought is in another place in Saint Vincent and the Grenadines

and that such computer data is lawfully accessible from or available to the first computer system, the police officer may extend the search and seizure to the other computer system.

(3) In the execution of a warrant under this section, a police officer may, in addition to the powers conferred on him by the warrant –

(a) activate an onsite computer system or computer data storage medium;

(b) make and retain a copy of computer data;

(c) remove computer data in a computer system or render it inaccessible;

(d) take a printout or output of computer data;

(e) impound or similarly secure a computer system or part of it or a computer data storage medium; or

(f) remove a computer system or computer data storage medium from its location.

(3) The police officer who undertakes a search under this section shall secure any apparatus and maintain the integrity of any computer data that is seized.

Assistance

34. (1) A person who has knowledge about the functioning of the computer system or measures applied to protect the computer data stored in the computer system that is the subject of a search warrant shall, if requested by the police officer authorized to undertake the search, assist the police officer by –

(a) providing information that facilitates the search for and seizure of the apparatus and computer data sought;

(b) accessing and using an apparatus to search computer data which is stored in, or lawfully accessible from or available to, that system;

(c) obtaining and copying the computer data; and

(d) obtaining an intelligible output from an apparatus in a format that is admissible for the purpose of legal proceedings.

(2) A person who fails to comply with this section commits an offence and is liable, on conviction, to a fine of one hundred thousand dollars or imprisonment for two years or to both.

Institution of criminal prosecution

35. A prosecution for an offence under this Act shall be instituted by, or with the written consent of, the Director of Public Prosecutions.

Arrest with warrant

36. A police officer not below the rank of superintendent may, with a warrant, arrest a person reasonably believed of committing an offence under this Act.

Extraditable offences;

Cap. 175

37. An offence under Part II is an extraditable offence for which extradition may be granted or obtained under the Fugitive Offenders Act.

PART IV

LIABILITY OF INTERNET SERVICE PROVIDERS

No monitoring obligation

38. (1) Subject to subsection (2), an internet service provider who provides a conduit for the transmission of information, is not responsible for –

(a) monitoring the information which it transmits or stores on behalf of another person in order to ascertain whether its processing would constitute or give rise to liability under this Act; or

(b) actively seeking facts or circumstances indicating illegal activity in order to avoid liability under this Act.

(2) Subsection (1) does not relieve an internet service provider from complying with any court order, injunction, writ or other legal requirement, which obliges an internet service provider to terminate or prevent an infringement based on any written law.

Access provider

39. (1) An access provider is not liable under this Act for providing access and transmitting information if the access provider does not–

(a) initiate the transmission;

(b) select the receiver of the transmission; or

(c) select or modify the information contained in the transmission.

(2) For the purpose of this section –

"access provider" means a person who provides a service to facilitate the transmission of computer data between two or more computer systems by transmitting information provided by or to a user of the service in a communication network or provides access to a communication network;

"communication network" means a set of devices or nodes connected by communication links, which is used to provide for the transfer of computer data between users located at various points or other similar services; and

"transmit" or "provide access" includes the automatic, intermediate and transient storage of information transmitted in so far as it takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for a period longer than is reasonably necessary for the transmission.

Hosting provider

40. (1) A hosting provider is not liable under this Act for the storage of information in contravention of this Act if –

(a) the hosting provider expeditiously removes or disables access to the information after receiving an order from a court to remove specific illegal information stored; or

(b) upon obtaining knowledge or awareness about specific illegal information stored by other ways than an order from a court, the hosting provider expeditiously informs the Attorney-General to enable the Attorney-General to evaluate the nature of the information and if necessary apply to a court for an order to remove the content.

(2) This section shall not apply when the user of the service is acting under the authority or the control of the hosting provider.

(3) If the hosting provider removes information after receiving an order under subsection (1) he is exempted from contractual obligations with his customer to ensure the availability of the service.

(4) For the purpose of this section –

"hosting provider" means a person who provides a service to facilitate the transmission of computer data between two or more computer systems by storing information provided by a user of his service.

Caching provider

41. (1) A caching provider is not liable for the storage of information in contravention of this Act if the caching provider –

(a) does not modify the stored information;

(b) complies with conditions of access to the stored information;

(c) updates stored information in accordance with any written law or in a manner widely recognized and used in the information communication technology industry;

(d) does not interfere with the lawful use of technology, widely recognized and used by the information communication technology industry, to obtain data on the use of the information; and

(e) acts expeditiously to remove or to disable access to the information the caching provider has stored upon obtaining knowledge of the fact that –

(i) the stored information at the initial source of the transmission has been removed from the network;

(ii) access to the stored information has been disabled; or

(iii) a court has ordered the removal or disablement of the stored information.

(2) For the purposes of this section –

"caching provider" means a person who provides a service to facilitate the transmission of computer data between two or more computer systems by the automatic, intermediate and temporary storage of information, where such storage is for the sole purpose of making the onward transmission of the information to other users of the service more efficient.

Hyperlinks provider

42. (1) A provider who enables the access to information provided by another person by providing an electronic hyperlink is not liable for the information that is in contravention of this Act if the provider–

(a) expeditiously removes or disables access to the information after receiving an order from a court to remove the link; or

(b) upon obtaining knowledge or awareness, by ways other than an order from a court, expeditiously informs the Attorney-General to enable the Attorney General to evaluate the nature of the information and if necessary apply to a court for an order to remove the content.

(2) For the purposes of this section –

"hyperlink" means a characteristic or property of an element such as a symbol, word, phrase, sentence, or image that contains information about another source and points to and causes to display another document when executed.

Search engine provider

43. A provider who operates a search engine that either automatically or based on entries by others, creates an index of internet-related content or, makes available electronic tools to search for information provided by another person, is not liable under this Act for the search results on condition if the provider –

(a) does not initiate the transmission;

(b) does not select the receiver of the transmission; or

(c) does not select or modify the information contained in the transmission.

PART V

MISCELLANEOUS

Regulations

44. The Minister may make regulations for the purpose of prescribing all matters that are required to be prescribed under this Act and for such other matters as may be necessary for giving full effect to this Act and for its proper administration.

SCHEDULE

(section 27)

OFFENCES

1. Treason.
2. High Treason.
3. Murder.
4. Manslaughter.
5. Offences involving abduction or kidnapping.
6. Drug trafficking, namely –
   (a) offences under the Drugs (Prevention of Misuse) Act;
   (b) offences under the Drug Trafficking Offences Act.
7. Unlawful possession of a firearm or ammunition.
8. Offences under the Anti-Terrorist and Proliferation Act 2015.
9. Offences under the Proceeds of Crime Act 2013.
10. Offences under the Prevention of Trafficking in Persons Act 2011.
11. Offences involving child pornography.
12. Offences involving fraud.

Passed in the House of Assembly this day of 2016.

Clerk of the House of Assembly.

OBJECTS AND REASONS

This Bill seeks to provide for the creation of offences related to cybercrimes and for related matters. For the most part, the offences created and the procedural mechanisms are derived from the Budapest Convention on Cybercrime.

Dr. the Hon. Ralph Gonsalves
Prime Minister, Minister of Finance
National Security, Legal Affairs, Grenadines Affairs and the Public Service