No. of 2019

VIRGIN ISLANDS

COMPUTER MISUSE AND CYBERCRIME (AMENDMENT) ACT, 2019

ARRANGEMENT OF SECTIONS

Section

1. Short title.
2. Section 2 amended.
3. Section 4 amended.
4. Section 7 amended.
5. Section 11 amended.
6. Section 14 amended.
7. Sections 14A to 14H inserted.
8. Sections 14I to 14S inserted.
9. Section 17A inserted.

No. of 2019 **Computer Misuse and Cybercrime (Amendment) Act, 2019** **Virgin Islands**

I Assent

Governor.

VIRGIN ISLANDS

No. of 2019

A Bill for

An Act to amend the Computer Misuse and Cybercrime Act, 2014 (No.9 of 2014).

[Gazetted , 2019]

ENACTED by the Legislature of the Virgin Islands as follows:

Short title.

1. This Act may be cited as the Computer Misuse and Cybercrime (Amendment) Act, 2019.

Section 2 amended. No.9 of 2014

2. The Computer Misuse and Cybercrime Act, 2014 (referred to in this Act as "the principal Act") is amended in section 2 by

(a) inserting in their proper alphabetical order, the following definitions:

""mobile phone tracking" means the tracking of the current position of a mobile phone and includes location based services that discloses the actual coordinates of a mobile phone bearer;

"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 a computer;

(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 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 a computer, generated by a computer 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;".

(b) replacing the definition of "computer service" with the following:

"computer service" includes provision of access to any computer or to any function of a computer, computer output, data processing and the storage or retrieval of data;".

Section 4 amended.

3. Section 4 of the principal Act is amended by replacing subsection (3) with the following:

"(3) A person who commits an offence under subsection (1) is liable

(a) summary conviction to a fine not exceeding two hundred thousand dollars or to imprisonment for a term not exceeding seven years, or both; or

(b) conviction on indictment to a fine not exceeding five hundred thousand dollars or to imprisonment for a term not exceeding fourteen years, or both.".

Section 7 amended.

4. Section 7 of the principal Act is amended by replacing subsection (3) with the following:

"(3) A person who commits an offence under subsection (1) is liable

(a) summary conviction to a fine not exceeding two hundred thousand dollars or to imprisonment for a term not exceeding seven years, or both; or

(b) conviction on indictment to a fine not exceeding five hundred thousand dollars or to imprisonment for a term not exceeding fourteen years, or both.".

Section 11 amended.

5. Section 11 of the principal Act is amended by replacing subsection (2) with the following:

"(3) A person who commits an offence under subsection (1) is liable

(a) summary conviction to a fine not exceeding two hundred thousand dollars or to imprisonment for a term not exceeding seven years, or both; or

(b) conviction on indictment to a fine not exceeding five hundred thousand dollars or to imprisonment for a term not exceeding fourteen years, or both.".

Section 14 amended.

6. Section 14(1) of the principal Act is amended

(a) by replacing the words "child pornography" with the words "child abuse material" wherever they appear;

(b) in subsection (1),

(i) in paragraph (b), by deleting the word "or";

(ii) in paragraph (c), by replacing the full stop at the end thereof with a semicolon; and

(iii) by inserting after paragraph (c) the following new paragraphs:

"(d) cultivate, entice or induce a child to an online relationship with another child or an adult on a computer, for a sexually explicit act or in a manner that may offend a reasonable adult;

(e) facilitate abusing a child online; or

(f) record in an electronic form own abuse or that of others pertaining to sexually explicit act with a child.".

(c) by replacing subsection (5) (a), with the following:

"(a) "child abuse material" includes audio recordings, and material that visually depicts

(i) a child engaged in sexually explicit conduct,

(ii) a person who appears to be a child engaged in sexually explicit conduct, and

(iii) a child in the nude or in a sexually explicit manner,

and "child" has the meaning provided in section 2 of the Children and Young Persons Act, 2005; and".

Sections 14A to 14H inserted.

7. The principal Act is amended by inserting after section 14 the following new sections:

"Sending offensive messages through a computer.

14A. (1) A person commits an offence if he or she sends by means of a computer

(a) information that is grossly offensive or has menacing character;

(b) information which he or she knows is false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer; or

(c) electronic mail or an electronic message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages.

(2) For the purpose of this section, the term "electronic mail" or "electronic message" means a message or information created or transmitted or received on a computer including attachments in text, images, audio, video and any other electronic record which may be transmitted with the message.

(3) A person who commits an offence under subsection (1) is liable

summary conviction to a fine not exceeding two hundred thousand dollars or to imprisonment for a term not exceeding seven years, or both; or

conviction on indictment to a fine not exceeding five hundred thousand dollars or to imprisonment for a term not exceeding fourteen years, or both.

Electronic defamation.

14B. (1) A person commits an offence if he or she defames another person using a computer.

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

Electronic forgery.

14C. (1) A person commits an offence if he or she intentionally and unlawfully interfere with a computer or data held in a computer with the intention that the computer or the data is used to induce a person to accept the data held in the computer 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 commits an offence under subsection (1) is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years, or both.

Electronic fraud.

14D. (1) A person commits an offence if he or she for gain, interferes with data or a computer

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

(b) with intent to deceive a person,

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

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

Misuse of encryption.

14E. (1) A person commits an offence if he or she for the purpose of the commission of an offence or concealment of incriminating evidence, knowingly and willfully encrypts any incriminating communication or data contained in a computer relating to the offence or incriminating evidence.

(2) A person who commits an offence under

subsection (1) is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years, or both.

Electronic stalking.

14F. (1) A person commits an offence if he or she, with intent to harass, intimidate, torment, or embarrass any other person, communicates by computer to such person or to a third party

(a) using any lewd, lascivious, indecent, or obscene words, images, or language, or suggesting the commission of any lewd or lascivious act anonymously or repeatedly whether or not conversation occurs; or

(b) threatening to inflict injury on the person or property of the person communicated with or any member of his or her family or household.

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

summary conviction to a fine not exceeding two hundred thousand dollars or to imprisonment for a term not exceeding seven years, or both; or

conviction on indictment to a fine not exceeding five hundred thousand dollars or to imprisonment for a term not exceeding fourteen years, or both.

(3) An offence committed under this section may be deemed to have been committed either at the place from which the communication was made or at the place where the communication was received.

Spoofing.

14G. (1) A person commits an offence if he or she establishes a website or send an electronic message with a counterfeit source

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

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

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

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

Violation of privacy.

14H. (1) A person commits an offence if he or she, knowingly or without lawful excuse or justification, captures, publishes or transmits an image of a private area of another person, without his or her consent, under circumstances violating the privacy of that person.

(2) A person commits an offence if he or she, knowingly or without lawful excuse or justification, captures, publishes or transmits an image of a private area of a mentally or physically impaired person.

(3) A person who commits an offence under subsections (1) or (2) is liable

(a) on summary conviction to a fine not exceeding two hundred thousand dollars or to a term of imprisonment not exceeding seven years or to both; or

(b) on conviction on indictment to a fine not exceeding five hundred thousand dollars or to a term of imprisonment not exceeding fourteen years or to both.

(2) For the purposes of this section

(a) "capture" means to videotape, photograph, film or record by any means;

(b) "private area" means the naked or undergarment clad genitals, pubic area, buttocks, or female breast;

(c) "publishes" means reproduction in the printed or electronic form and making it available publicly;

(d) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

(e) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that

(i) he or she could disrobe in privacy, without being concerned that an image or his or her private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.".

Sections 14I to 14S inserted.

8. The principal Act is amended by inserting the following new heading and sections:

"INVESTIGATIONS AND PROCEDURES

Preservation order.

14I. (1) A police officer may apply to a court for an order for the expeditious preservation of data that has been stored or processed by means of a computer, 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) shall remain 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 court determines necessary.

Disclosure of preserved data order.

14J. (1) A police officer may, for the purposes of a criminal investigation or the prosecution of an offence, apply to a court for an order for the disclosure of

(a) any preserved data, irrespective of whether one or more service providers 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.

(2) For the purposes of this section, "electronic key" in relation to any data or other computer output, means any code, password, algorithm or other data the use of which (with or without other keys)

(a) allows access to the data or output; or

(b) facilitates the putting of the data or output into intelligible form;

Production order.

14K. (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 court for an order compelling

(a) a person to submit specified data in that person's possession or control, which is stored in a computer;

(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 a computer, 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, audible, and legible as relevant.

(3) A person or service provider who refuses to produce the information under subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred thousand dollars.

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

14L. (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 court 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 a police officer shall include the power to

(a) access, inspect and check the operation of a computer;

(b) use or cause to be used a computer to search any data contained in or available on the computer;

(c) access any information, code or technology which has the capability of transforming or unscrambling encrypted data contained or available to a computer 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 a person in possession of the decryption information to grant the police officer access to such decryption information necessary to decrypt data required for the purpose of investigating the offence;

(e) seize or secure a computer.

(3) In the execution of a warrant under subsection (1), a police officer may be accompanied by professionals or experts as necessary to carry out the technical aspects of the search and seizure of the data.

(4) A person commits an offence if he or she knowingly or without lawful excuse

(a) obstructs a police officer in the exercise of the police officer's powers under this section; or

(b) fails to comply with a request made by a police officer under this section.

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

Real time collection of traffic data.

14M. 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, the police officer may apply to a court for an order

(a) allowing the collection or recording of traffic data, in real time, associated with specified communications transmitted by means of a computer; 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.

Mobile phone tracking in emergencies.

14N. (1) A mobile phone service provider shall provide mobile phone tracking to the law enforcement agencies upon request in cases of emergencies with respect to the mobile phone of a person involved in such emergency.

(2) For the purposes of this section, "cases of emergency" include road accidents, missing persons and the pursuit of suspects involved in murder, rape or kidnapping.

(3) A mobile phone provider who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding twenty five thousand dollars.

Record of and access to seized items.

14O. (1) Where any computer or data is seized or rendered inaccessible in the execution of a warrant under section 14K, the person who executed the warrant shall, at the time of the search, or as soon as possible thereafter

(a) make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and

(b) give a copy of the list to the person to whom the warrant is addressed or the occupier of the premises on which the warrant is executed,

(2) Subject to subsection (3), the police officer who executed the warrant or another authorised person shall, on request,

(a) permit a person who had the custody or control of the computer or data, or someone acting on their behalf to access and copy data on the computer data on the; or

(b) give the person a copy of the data.

(3) The police officer or authorised person may refuse to give access or provide copies of the data if he or she has reasonable grounds for believing that giving access, or providing the copies would

(a) constitute a criminal offence; or

(b) prejudice

(i) the investigation in relation to which the warrant was issued;

(ii) another ongoing investigation; or

(iii) any criminal proceedings that may be brought in relation to any investigation referred in subparagraph (i) or (ii).

Arrest without warrant.

14P. A police officer may, without a warrant, arrest a person reasonably suspected of committing an offence under this Act.

Deletion.

14Q. A court may, on application by a police officer and on being satisfied that a computer contains indecent data order that the indecent data be

(a) no longer stored on or be made available through the computer; or

(b) deleted or destroyed; and

(c) recorded and preserved by the police for the purposes of prosecution.

Limited use of data and information.

14R. A person shall not use or disclose data obtained pursuant to sections 14I, 14J, 14K, 14L, 14M and 14N 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 court;

(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.

Limitation of liability for service provider.

14S. (1) A service provider shall not be liable for any actions taken or any information provided or disclosed to the Police or other law enforcement agencies in accordance with sections 14I, 14J, 14K, 14L, 14M and 14N.

(2) A service provider who without lawful authority discloses

(a) the fact that an order under this Act has been made; or

(b) anything done under the order; or

(c) any data collected or recorded under the order,

commits an offence and is liable on conviction on indictment to a fine not exceeding fifty thousand dollars or to imprisonment for a term not exceeding five year, or both.".

Section 17A inserted.

9. The principal Act is amended by inserting immediately after section 17 the following new section:

"Forfeiture.

17A. (1) Where a person is convicted of an offence under this Act the court may, in addition to any penalty imposed on the person, 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 be stored or made available through the computer.".

Passed by the House of Assembly this day of , 2019.

Speaker.

Clerk of the House of Assembly.

OBJECTS AND REASONS

This Bill seeks to amend the Computer Misuse and Cybercrime Act, 2014 (No.9 of 2014) (referred to in this Act as "the principal Act").

Clause 1 sets out the short title.

Clause 2 would amend section 2 of the principal Act by inserting several new definitions.

Clause 3, 4 and 5 would amend sections 4, 7 and 11 of the principal Act by increasing the fines and penalties provided for in those sections.

Clause 6 would amend section 14 of the principal Act by inserting new paragraphs which would make it an offence to induce a child into certain relationships online, facilitate abuse of a child online and record the abuse of a child online. It would also replace the words "child pornography" with the words "child abuse materials".

Clause 7 would insert sections 14A to 14H which would provide for several new offences including sending of offensive messages through a computer, electronic fraud, misuse of encryption, electronic stalking, spoofing and violation of privacy.

Clause 8 would insert a new heading comprising sections 14I to 14S which would provide for investigations and procedures of electronic crimes. Clauses 14I to 14K would provide for the grant of a preservation order, disclosure of preserved data order and production order by a court on the application of a police officer. Clause 14L would provide for a police officer to apply to the court for the issue of a warrant that enables the police officer to access, search and seize stored data that would be relevant for the purposes of an investigation or the prosecution of an offence. Clause 14M would provide for a police officer to apply to the court for an order collect or record traffic data in real time. Clause 14N would provide that a mobile phone provider shall provide mobile phone tracking to law enforcement agencies in cases of emergencies. The term "cases of emergencies: is defined to include road accidents, missing persons and the pursuit of suspects involved in murder, rape or kidnapping. Clause 14O would provide for a record to be kept of any computer or data seized and for access to be granted to those items. Clause 14P would provide for arrests without a warrant where a person is reasonably suspected of committing an offence under the Act. Clause 14Q would provide for the deletion of indecent material be deleted from a computer. Clause 14R would provide for limited use of the data obtained and sets out the exception to that rule. Clause 14S would provide for the limitation of liability for service that a service provider

Clause 9 would insert a new section 17A which would provide for forfeiture of any apparatus, article or thing used in connection with the commission of an offence under the Act.

Minister for Finance.