ANTIGUA AND BARBUDA

ELECTRONIC CRIMES ACT, 2013

No. 14 of 2013

[Published in the Official Gazette Vol. XXXIII No. 65 dated 14th November, 2013]

Printed at the Government Printing Office, Antigua and Barbuda,
by Ralph George, Government Printer
— By Authority, 2013.

600—11.13 *[Price $ 7.85]*

ELECTRONIC CRIMES ACT, 2013

ARRANGEMENT OF CLAUSES

32. Conflict of laws

Where a provision of this Act conflicts with any other enactment of Antigua and Barbuda, this Act shall prevail to the extent of the inconsistency.

Passed the House of Representatives on the 28th August, 2013.

D. Gisele Isaac-Arrindell,
Speaker.

Romona Small,
Clerk to the House of Representatives.

Passed the Senate on the 11th September, 2013.

Hazlyn M. Francis,
President.

Romona Small,
Clerk to the Senate.

(b) be attributable to the failure of any such director, manager, secretary, or other officer or person, to exercise all such reasonable diligence as he ought in the circumstances to have exercised to prevent the offence, having regard to the nature of his powers and all the circumstances,

the director, manager, secretary or other officer or person as aforesaid, as well as the body corporate commit that offence, and shall be liable to be proceeded against and punished accordingly.

(3) For the purposes of this section, a person shall be deemed to be a director of a body corporate if he occupies in relation thereto, the position of a director, by whatever name called, or is a person in accordance with whose directions or instructions (not being directions or instructions in a professional capacity only) the directors and the body corporate or any of them, act.

28. Extraditable offences

An offence pursuant to Part II shall be considered to be an extraditable crime for which extradition may be granted or obtained under the Extradition Act 1993.

29. Order for compensation

(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 a sum of money fixed by the Court by way of compensation to a person for damage caused to his or her electronic 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.

30. Forfeiture

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

(2) In addition to making an order that any 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.

31. Regulations

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

[L.S.]

I Assent,

Louise Lake-Tack,
Governor-General.

28th October, 2013.

ANTIGUA AND BARBUDA

ELECTRONIC CRIMES ACT, 2013

No. 14 of 2013

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 and consent of the Senate and House of Representatives of Antigua and Barbuda, and by the authority of the same as follows –

PART I
PRELIMINARY

1. Short title

This Act may be cited as the Electronic Crimes Act, 2013.

2. Interpretation

In this Act –

"access" in the context of an 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;

"child pornography" means pornographic material that depicts, presents or represents-

(a) a child engaged in sexually explicit conduct; or

(b) an image representing a child engaged in sexually explicit conduct;

“contaminant" means a set of electronic instructions that are designed to modify, destroy, record, transmit data or program residing within an electronic system; or by any means to take over the normal operation of an electronic system or electronic network;

“damage” includes modifying, altering, deleting, erasing, suppressing, changing location or making data temporarily unavailable, halting an 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 electronic program, 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;

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

"electronic database" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by an electronic system or electronic network and are intended for use in an electronic system or electronic network;

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

“electronic system” means an 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;

“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;

offences, apprehending or prosecuting offenders, assessing or collecting tax, duty or other monies owed or payable to 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.

25. No liability for service provider

(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 this Part.

(2) A service provider who without lawful authority discloses-

(a) the fact that an order under this Part was made; and

(b) any action taken or data collected or recorded under the Order, commits a summary offence and is liable on conviction to a fine not exceeding two hundred thousand dollars.

PART IV
MISCELLANEOUS

26. Institution of criminal proceedings

Criminal proceedings shall not be instituted under this Act except with the consent of, the Director of Public Prosecutions.

27. General penalty for Body Corporate

(1) Where an offence under this Act is committed by a body corporate, the body corporate shall be liable upon–

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

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

(2) Where an offence under this Act committed by a body corporate is proved to–

(a) have been committed with the consent or connivance of any director, manager, secretary, or other similar officer of the body corporate or any person who was purporting to act in that capacity; or

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

21. Mobile phone tracking in emergencies

(1) A mobile phone service provider shall provide mobile phone tracking to the Royal Police Force of Antigua and Barbuda upon request in cases of emergencies with respect to the mobile phone of a person involved in such emergency.

(2) For the purpose of this section, "cases of emergency" include cases of accidents, missing persons and the pursuit of suspects involved in murder, rape, kidnapping or any indictable offence punishable by at least five years imprisonment or more.

(3) A mobile phone provider who contravenes subsection (1) commits a summary offence and is liable on conviction to a fine of twenty five thousand dollars.

22. Arrest without warrant

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

23. Deletion

A Magistrate/Judge in Chambers may, on application by a police officer and being satisfied that an electronic system contains data that contains 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.

24. Limited use of data and information

A person shall not intentionally, without lawful excuse or justification 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 Magistrate/ Judge in Chambers;

(c) where the data is required for the purpose of preventing, detecting or investigating

"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 an electronic system;

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

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

"source code" means the listing of programs, electronic commands, design and layout and program analysis of an electronic system in any form;

"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 there to 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 a person to an electronic system or data held in an electronic system which is unauthorized or done without authority or is 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 a person so entitled.

PART II
OFFENCES

3. Access and interference

(1) A person shall not intentionally, without lawful excuse or justification,–

(a) access an electronic system or network;

(b) download, copy or extract data, electronic database or information from such electronic system or network including information or data held or stored in a removable storage medium;

(c) introduce or cause to be introduced a contaminant or malicious code into an electronic system or network;

(d) damage or cause to be damaged an electronic system or network, data, electronic data base or other program residing in such electronic system or network;

(e) disrupt or causes disruption of an electronic system or network;

(f) deny or cause the denial of access to a person authorised to access an electronic system or network by any means;

(g) provide assistance to a person to facilitate access to an electronic system or network in contravention of the provisions of this Act;

(h) charge the services availed of by a person to the account of another person by tampering with or manipulating an electronic system or network;

(i) willfully destroy, delete or alter information residing in an electronic system or diminish its value or utility, or affect it injuriously by any means; or

(j) steal, conceal, destroy or alter or cause a person to steal, conceal, destroy or alter any source code used for an electronic system with an intention to cause damage.

(2) A person who contravenes subsection (1) commits an offence and is liable on-

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

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

(b) use or cause to be used an electronic system to search any data contained in or available to the electronic 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 a 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 intentionally, without lawful excuse or justification –

(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 (3) commits a summary offence and is liable on conviction to a fine not exceeding fifty thousand dollars or to imprisonment for a term not exceeding twelve months, or both.

(5) For the purposes of this section–

"decryption information" means information or technology that enables a person to readily re-transform 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; and

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

20. Real time collection of traffic data

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 Magistrate/Judge in Chambers for an Order–

(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.

18. Production order

(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 Magistrate/Judge in Chambers for an Order compelling–

(2) If the disclosure of data is required for the purpose of a criminal investigation or the prosecution of an offence, a police officer shall make a request of–

(a) a person to submit specified data in that person's possession or control, which is stored in an electronic 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.

(3) 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, audible or legible.

(4) A person or service provider who refuses to produce the information under subsection (1) commits an offence and is liable on summary conviction to a fine of one hundred thousand dollars or to imprisonment not exceeding twelve months, or to both.

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

(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 Magistrate/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 an electronic system;

4. Sending offensive messages through communication services, etc

(1) A person shall not intentionally, without lawful excuse or justification send by means of an electronic system –

(a) information that is offensive or threatening;

(b) information which is false, causing annoyance, inconvenience, danger, obstruction, insult, injury, intimidation, enmity, hatred or ill will, persistently by making use of such electronic system or an electronic device; or

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

(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 an electronic system or electronic device including attachments in text, images, audio, video and any other electronic record which may be transmitted with the message.

(3) A person who contravenes subsection (1) commits an offence and is liable on-

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

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

5. Identify theft

(1) A person shall not intentionally, without lawful excuse or justification make fraudulent or dishonest use of an electronic signature, password or other unique identification feature of another person.

(2) A person who contravenes subsection (1) commits an offence and is liable on-

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

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

6. Electronic forgery

A person who, with intent to defraud, inputs, alters, deletes, or suppresses computer data, resulting in inauthentic data, whether or not the data is directly readable and intelligible, commits an offence and is liable on-

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

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

7. Electronic fraud

(1) A person shall not, intentionally or without lawful excuse or justification, induce another person to enter into a relationship, with the intent to defraud that person or cause that person to act to his own detriment or suffer loss of property, by –

(a) any input, alteration, deletion or suppression of data; or

(b) any interference with the functioning of an electronic system.

(2) A person who contravenes subsection (1) commits an offence and is liable on-

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

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

8. Violation of privacy

(1) Subject to subsection (2), a person who, intentionally or without lawful excuse or justification, captures, publishes or transmits the image of a private area of a person, or the image whether whole or partial of a person in a vulnerable position without his or her consent, under circumstances violating the privacy of that person, commits an offence and is liable on –

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

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

(2) A person who commits an offence under subsection (1) is liable to face the same penalty specified in that subsection, where the victim of the offence is disabled or mentally incapacitated and incapable of giving his or her consent.

(3) For the purposes of this section–

"capture" with respect to an image, means to videotape, photograph, film or record by any means;

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

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

15. Unauthorised access to code

(1) A person shall not intentionally, without lawful excuse or justification disclose or obtain a password, an access code or any other means of gaining access to an electronic system or data with intent to obtain wrongful gain or inflict wrongful loss to a person or for any unlawful purpose.

(2) A person who contravenes subsection (1) commits an offence and is liable on-

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

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

PART III
INVESTIGATIONS AND PROCEDURES

16. Preservation order

(1) A police officer may apply to a Magistrate/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 Magistrate/Judge in Chambers determines necessary.

17. Disclosure of preserved data order

A police officer may, for the purposes of a criminal investigation or the prosecution of an offence, apply to a Magistrate/Judge in Chambers for an Order for the disclosure of–

to cause injury to the interests of the sovereignty of Antigua and Barbuda, the security of Antigua and Barbuda, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise,

commits an indictable offence of electronic terrorism and is liable on conviction pursuant to the penalties prescribed pursuant to the Prevention of Terrorism Act 2005.

13. Harassment utilizing means of electronic system

A person shall not intentionally, without lawful excuse or justification intimidate, coerce or harass another person using an electronic system commits an offence and is liable on –

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

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

14. False websites and Spam

(1) A person shall not intentionally, without lawful excuse or justification set up 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 a 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 shall not intentionally without lawful excuse or justification –

(a) initiate the transmission of multiple electronic mail messages from or through an electronic system;

(b) use a protected computer system to relay or retransmit multiple electronic mail messages, with the intent to deceive or mislead users, or any electronic mail or internet service provider, as to the origin of such messages; or

(c) materially falsify header information in multiple electronic mail messages and initiate the transmission of such messages.

(3) A person who contravenes subsection (1) or (2) commits an offence and is liable on –

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

"publishes" means reproduction in the printed or electronic form and making it available for public;

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

"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 of 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.

"vulnerable position" means circumstances in which a person is ill, injured or otherwise physically incapacitated.

9. Misuse of encryption

(1) A person shall not intentionally, without lawful excuse or justification for the purpose of commission of an offence or concealment of incriminating evidence, intentionally 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-

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

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

10. Child pornography

(1) For the purposes of this section a "child" means a person who is under the age of eighteen years.

(2) A person shall not intentionally without lawful justification or excuse–

(a) publish, transmit or cause to be published or transmitted material in an electronic form which depicts a child engaged in a sexually explicit act or conduct;

(b) create text or digital images, collect, seek, browse, download, advertise, promote, exchange or distribute material in an electronic form depicting a child in an obscene or indecent or sexually explicit manner;

(c) cultivate, entice or induce a child into an online relationship with another child or an adult for a sexually explicit act or in a manner that may offend a reasonable adult on an electronic system;

(d) facilitate the abuse of a child online;

(e) record or own in an electronic form material which depicts the abuse of a child engaged in a sexually explicit act;

(f) procure or obtain child pornography through a computer system; or

(g) obtain access through information and communication technologies, to child pornography.

(3) It is a defence to a charge of an offence under subsection (2) paragraphs *(f)* and *(g)* where the person can establish that the child pornography was for a bona fide law enforcement purpose.

(4) A person who contravenes subsection (2) commits an offence and is liable on-

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

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

(5) Subsection (2) does not apply to a book, pamphlet, paper, drawing, painting, representation or figure or writing in an electronic form–

(a) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or

(b) which is kept or used for bona fide heritage or religious purposes.

11. Sensitive electronic system

(1) A person shall not intentionally, without lawful excuse or justification 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 (1) commits an indictable offence and is liable on

conviction to a fine not exceeding three hundred thousand dollars or to imprisonment for a term not exceeding twenty years or to both.

(3) For the purposes of this section a "sensitive electronic system" is an electronic system used directly in connection with or necessary for–

(a) the security, defence or international relations of Antigua and Barbuda ;

(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.*

12. Electronic terrorism

A person who–

(a) with intent to threaten the peace, security or sovereignty of Antigua and Barbuda or to strike terror in the people or any section of the people by–

(i) denying or causing the denial of access to any person authorised to access an electronic system;

(ii) attempting to penetrate or access an electronic system without authorisation or exceeding authorised access; or

(iii) introducing or causing to introduce any contaminant into an electronic system,

and by means of such conduct causes or is likely to cause death or injury to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure relating to the security of Antigua and Barbuda, or

(b) intentionally penetrates or accesses an electronic system without lawful authorization and by means of such conduct obtains access to information, data or electronic database that is restricted for reasons for the security of Antigua and Barbuda or foreign relations, or any restricted information, data or electronic database, with reasons to believe that such information, data or electronic database so obtained may be used to cause or likely