



The Official Gazette

(EXTRAORDINARY)

OF GUYANA

Published by the Authority of the Government

GEORGETOWN, MONDAY 13TH AUGUST, 2018

TABLE OF CONTENTS	PAGE
-------------------	------

FIRST SUPPLEMENT

LEGAL SUPPLEMENT

A.	ACTS —	
	Act No. 16 of 2018 – The Cybercrime Act 2018	275
B.	SUBSIDIARY LEGISLATION — NIL	
C.	BILLS — NIL	

GEORGETOWN, Demerara – Printed and Published every Saturday and on such Extraordinary Days as may be directed by the Government by Guyana National Printers Limited, 1 Public Road, La Penitence, Greater Georgetown.

MONDAY 13TH AUGUST, 2018

THE OFFICIAL GAZETTE 13TH AUGUST, 2018
LEGAL SUPPLEMENT — A



ACT NO. 16 OF 2018
CYBERCRIME ACT 2018

I assent.



David Granger,
President.

2018-08-13

ARRANGEMENT OF SECTIONS

SECTION

PART I
PRELIMINARY

1. Short title.
2. Interpretation.

PART II
CYBERCRIME OFFENCES

3. Illegal access to a computer system.
4. Illegal interception.
5. Illegal data interference.
6. Illegal acquisition of data.
7. Illegal system interference.
8. Illegal devices.
9. Unauthorised granting of access to or giving of electronic data.
10. Computer-related forgery.
11. Computer-related fraud.
12. Offences affecting critical infrastructure.
13. Identity-related offences.
14. Child pornography.
15. Child luring.
16. Publication or transmission of image of private area of a person.
17. Multiple electronic mail messages and fraudulent website.
18. Offences against the State.
19. Using a computer system to coerce, harass, intimidate, humiliate, etc. a person.
20. Infringement of copyright, patents and designs and trademarks.
21. Corporate liability.
22. Attempt, aiding or abetting.
23. Use of computer system to commit offence under any other law.
24. Offences prejudicing investigation.

PART III
ENFORCEMENT

25. Service providers to store traffic data and subscriber information.
26. Extension of time for prosecution of an offence.
27. Jurisdiction.
28. Search and seizure.

29. Record of seized material.
30. Assistance.
31. Production order.
32. Expedited preservation order.
33. Disclosure of traffic data order.
34. Confidentiality of order.
35. Prohibition of disclosures.
36. Protection of person aiding in enforcement of Act.
37. Order for removal or disablement of data.
38. Remote forensic tools.
39. Order for payment of compensation.
40. Forfeiture order.
41. Order for seizure and restraint regarding forfeiture.
42. Failure to comply with a court order.
43. Evidence.

AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences and related matters.

AD.2018

Enacted by the Parliament of Guyana:-

**PART I
PRELIMINARY**

Short title.

1. This Act may be cited as the Cybercrime Act 2018.

Interpretation.

2. In this Act –

“child” means a person under the age of eighteen years;

“child pornography”-

(a) means any visual depiction, including any film, video, digital image, computer or computer-generated or modified image, animation or text, of –

(i) a child engaging in real or simulated explicit sexual activity;

(ii) a child in a sexually explicit pose;

(iii) parts of a child’s body pasted, for sexual purposes, to visual representations of parts of an adult’s body or vice versa;

(b) does not include any visual representation of a child’s body produced or reproduced for the purpose of education, counselling, or promotion of reproductive health or as part of a criminal investigation and prosecution or civil proceedings or in the lawful performance of a person’s profession, duties and functions;

(c) does not require proof of the actual identity of a child;

“computer programme” means electronic data which

represents instructions or statements that, when executed in a computer system, can cause the computer system to perform a function;

“computer system” –

- (a) means a device or group of interconnected or related devices, which follows a computer programme or external instruction to perform automatic processing of electronic data; and
- (b) includes, but is not limited to, a desktop computer, a laptop computer, a netbook computer, a tablet computer, a video game console, internet connected devices, a smart phone, a personal digital assistant, a smart television or a video camera;

“electronic data”-

- (a) means any digital representation of—
 - (i) facts;
 - (ii) concepts;
 - (iii) machine-readable code or instructions; or
 - (iv) information, including text, audio, image or video,that is in a form suitable for processing in a computer system and is capable of being sent, received or stored; and

- (b) includes traffic data or a computer programme;

“electronic data storage medium” means anything –

- (a) in which electronic data is capable of being stored; or
- (b) from which electronic data is capable of being retrieved or reproduced,

with or without the aid of a computer system;

“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 system;

“intercept” includes –

- (a) listening to, viewing, or recording a function of a computer system; or
- (b) acquiring the substance, meaning or purport of a function of a computer system, by use of technical means, other than by the sender or an intended recipient;

“service provider” means-

- (a) any public or private entity that provides to users of its service the ability to communicate by means of a computer system; or
- (b) any public or private entity that processes or stores electronic data on behalf of such communication service or users of such service;

"sexual activity" includes –

- (a) touching with any part of the body, which includes a part surgically constructed (in particular, through gender reassignment surgery), with anything else or through anything; or
- (b) any other activity,

if a reasonable person would consider that –

- (i) whatever its circumstances or any person's purpose in relation to it, it is because of its nature sexual; or
- (ii) because of its nature it may be sexual and because of its circumstances or the purpose of any person in relation to it (or both) it is sexual; or
- (c) sexual intercourse;

“subscriber information” means any information contained in the form of electronic data or any other form that is held by a service provider, relating to subscribers of its services and by which can be established-

- (a) the type of communication service used, the technical provisions taken 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;
- (c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement;

“security measure” includes passwords, access codes and encryption codes, hardware and software programme configuration and update settings, and other controls to detect or prevent any cybercrime offence;

“traffic data” means electronic data that-

- (a) relates to a communication by means of a computer system;
- (b) is generated by a computer system that is part of a chain of communication; and
- (c) shows the communication’s origin, destination, route, time, date, size, geographic location, duration or the type of underlying services.

PART II
CYBERCRIME OFFENCES

Illegal access to a computer system.

3. (1) A person commits an offence if the person intentionally, without authorisation or in excess of authorisation, or by infringing any security measure, accesses a computer system or any part of a computer system of another person.

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

- (a) on summary conviction to a fine of three million dollars and to imprisonment for three years; or
- (b) on conviction on indictment to a fine of five million dollars and to imprisonment for five years.

Illegal interception.

4. (1) A person commits an offence if the person intentionally and without lawful excuse or justification, intercepts –

- (a) the transmission of electronic data or any communication of another person to, from or within a computer system; or
- (b) any electromagnetic emission carrying electronic data from a computer system.

(2) A person does not commit an offence under subsection (1) if –

- (a) the transmission is for use of the general public;
- (b) the person is a party to the transmission, or one of the parties to the transmission has provided consent to such interception;
- (c) the person is acting on behalf of a service provider and the interception either is necessary to provide the service, or to protect the rights and property of the service provider or its customers, consistent with the service provider's terms of reference;
- (d) the transmission is intercepted in obedience to a warrant issued by a Judge under section 6 of the Interception of Communications Act;
- (e) the transmission is intercepted under the Interception of

Communications Act on the authority of a designated officer in the case of a national emergency or in responding to a case where approval for a warrant is impracticable having regard to the urgency of the case;

- (f) for a lawful security purpose, the person intercepts a transmission that constitutes unauthorised access, or access in excess of authorisation, from a computer system owned by the person, or with the authorisation of the owner.
- (3) A person who commits an offence under subsection (1) is liable—
- (a) on summary conviction to a fine of five million dollars and to imprisonment for three years; or
 - (b) on conviction on indictment to a fine of eight million dollars and to imprisonment for five years.

Illegal data
interference.

5. (1) A person commits an offence if the person intentionally and without lawful excuse or justification—

- (a) causes electronic data of another person to deteriorate;
- (b) deletes electronic data of another person;
- (c) alters or modifies electronic data of another person;
- (d) copies or moves electronic data of another person to a different location within a computer system or to any electronic data storage medium;
- (e) renders electronic data of another person meaningless, useless or ineffective;
- (f) obstructs, interrupts or interferes with another person's lawful use of electronic data; or
- (g) denies access to electronic data to a person who is authorised to access it.

- (2) A person who commits an offence under subsection (1), is liable—
- (a) on summary conviction to a fine of three million dollars and to imprisonment for three years; or

(b) on conviction on indictment to a fine of eight million dollars and to imprisonment for five years.

Illegal acquisition of data.

6. A person who, intentionally and without lawful excuse or justification, acquires electronic data of another person commits an offence and is liable—

- (a) on summary conviction to a fine of three million dollars and to imprisonment for three years; or
- (b) on conviction on indictment to a fine of eight million dollars and to imprisonment for five years.

Illegal system interference.

7. (1) A person commits an offence if the person intentionally and without lawful excuse or justification, hinders or interferes with —

- (a) a computer system of another person; or
- (b) another person's lawful use or operation of a computer system.

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

- (a) on summary conviction to a fine of three million dollars and imprisonment for three years; or
- (b) on conviction on indictment to a fine of eight million dollars and imprisonment for five years.

(3) For the purposes of this section “hinder” includes—

- (a) disconnecting the electricity supply to a computer system;
- (b) causing electromagnetic interference to a computer system;
- (c) corrupting a computer system; or
- (d) damaging, deleting, deteriorating, altering or suppressing computer programme.

Illegal devices.

8. (1) A person commits an offence if the person intentionally and without lawful excuse or justification, possesses, procures for use, produces, sells, imports, exports, distributes, discloses or otherwise makes available —

- (a) a device or a computer programme, that is designed or adapted; or
- (b) a computer password, access code, encryption code or similar data by which the whole or any part of a computer system, electronic data storage medium or electronic data is capable of being accessed,

for the purpose of committing an offence under this Act or any other law.

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

- (a) on summary conviction to a fine of three million dollars and to imprisonment for three years; or
- (b) on conviction on indictment to a fine of eight million dollars and to imprisonment for five years.

Unauthorised granting of access to or giving of electronic data.

9. (1) A person commits an offence who, through authorised or unauthorised means, obtains or accesses electronic data which –

- (a) is commercially sensitive or a trade secret;
- (b) relates to the national security of the State; or
- (c) is stored on a computer system and is protected against unauthorised access,

and intentionally and without lawful excuse or justification grants access to or gives the electronic data to another person, whether or not he knows that the other person is authorised to receive or have access to the electronic data.

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

- (a) on summary conviction to a fine of three million dollars and to imprisonment for three years; or
- (b) on conviction on indictment to a fine of eight million dollars and to imprisonment for five years.

Computer-related forgery.

10. A person who inputs, alters, deletes or suppresses electronic data, resulting in inauthentic data, with the intent that it be considered or acted upon by another person as if it were authentic, regardless of whether or not

the data is directly readable and intelligible, commits an offence and is liable—

- (a) on summary conviction to a fine of three million dollars and to imprisonment for three years; or
- (b) on conviction on indictment to a fine of five million dollars and to imprisonment for five years.

Computer-related fraud.

11. (1) A person commits an offence if the person –

- (a) inputs, alters, deletes or suppresses electronic data; or
- (b) interferes with the functioning of a computer system,

with the intent to defraud or deceive another person for the purpose of procuring an economic benefit for himself or another person.

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

- (a) on summary conviction to a fine of five million dollars and to imprisonment for five years; or
- (b) on conviction on indictment to a fine of ten million dollars and imprisonment for ten years.

Offences affecting critical infrastructure.

12. (1) Notwithstanding the penalties set out in any other provision of this Act or any other law, where a person commits an offence under this Act or under any other law and the offence results in the incapacity or destruction of or interference with, electronic data, a computer system, or a computer network that—

- (a) is exclusively for the use of critical infrastructure of the State;
or
- (b) affects the use, or impacts the operation, of critical infrastructure of the State,

that person is liable on conviction on indictment to a fine of twenty million dollars and to imprisonment for ten years.

(2) For the purposes of this section, “critical infrastructure” means any electronic data, computer system, or computer network so vital to the

State that the incapacity or destruction of, or interference with, such electronic data, computer system, or computer network would have a debilitating impact on –

- (a) the security, defence or international relations of the State;
- (b) the existence or identity of a confidential source of information relating to the enforcement of the criminal law of the State;
- (c) the provision of services by the Office of the Director of Public Prosecutions and the Ministry of Legal Affairs;
- (d) confidential educational material, such as examination materials;
- (e) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or essential public infrastructure such as hospitals, courts, traffic lights, bridges, airports and seaports;
- (f) the protection of public safety, including systems related to essential emergency services such as police, fire brigade services, civil defence and medical services;
- (g) the provision of services of the Revenue Authority established under the Revenue Authority Act; or
- (h) the provision of services of the Bank of Guyana.

Cap. 79:04

Identity-related offences.

13. (1) A person commits an offence if the person uses a computer system to –

- (a) transfer, possess or use a means of identification of another person; or
- (b) make use of the electronic signature or password of another person,

with the intent to commit an offence under this Act or under any other law.

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

- (a) on summary conviction to a fine of five million dollars and to imprisonment for three years; or
- (b) on conviction on indictment to a fine of eight million dollars and to imprisonment for five years.

Child pornography.

14. (1) A person commits an offence if the person intentionally –

- (a) produces child pornography with the use of a computer system;
- (b) offers or makes available, distributes or transmits child pornography through a computer system;
- (c) procures or obtains child pornography through a computer system for himself or another person; or
- (d) possesses child pornography in a computer system or on an electronic data storage medium.

(2) A person or a service provider who has knowledge of another person committing child pornography through a computer system shall report the commission of the child pornography to the Police.

(3) A person or a service provider who fails to comply with subsection (2) commits an offence.

(4) A person who commits an offence under subsection (1), or a person or a service provider who commits an offence under subsection (3), is liable –

- (a) on summary conviction to a fine of ten million dollars and to imprisonment for five years; or
- (b) on conviction on indictment to a fine of fifteen million dollars and to imprisonment for ten years.

Child luring.

15. (1) A person commits an offence if the person uses a computer system to -

- (a) communicate with a child with the intent to induce the child to engage in sexual conversations or sexual activities; or

(b) arrange a meeting with a child with the intent of abusing or engaging in sexual activity with the child or producing child pornography, whether or not he takes any steps to effect such a meeting.

(2) A person or a service provider who has knowledge of another person committing child luring through a computer system shall report the commission of the child luring to the Police.

(3) A person or service provider who fails to comply with subsection (2) commits an offence.

(4) A person who commits an offence under subsection (1), or a person or a service provider who commits an offence under subsection (3), is liable –

(a) on summary conviction to a fine of three million dollars and to imprisonment for five years; or

(b) on conviction on indictment to a fine of eight million dollars and to imprisonment for five years.

Publication or transmission of image of private area of a person.

16. (1) A person commits an offence if the person intentionally captures, stores in, publishes or transmits through a computer system, the image of the private area of another person without that other person's consent.

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

(a) on summary conviction to a fine of three million dollars and to imprisonment for three years; and

(b) on conviction on indictment to a fine of eight million dollars and to imprisonment for five years.

(3) For the purposes of this section, “private area” means naked genitals, buttocks or female breasts.

Multiple electronic mail messages and fraudulent website.

17. (1) A person commits an offence if the person –

(a) intentionally initiates the transmission of multiple

electronic mail messages from or through a computer system; or

- (b) with intent to deceive or mislead a recipient or service provider as to the origin of the message, uses a computer system to transmit or retransmit multiple electronic mail messages,

that causes harm to a person or damage to a computer system.

(2) A person commits an offence if the person intentionally falsifies the header information of an electronic mail message for the purpose of committing an offence under this Act or any other law.

(3) A person commits an offence if the person without lawful excuse or justification establishes a website, with the intent to deceive or mislead a visitor to the website as to the authenticity of the website, for the purpose of gaining unauthorised access to information to commit a further offence.

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

- (a) on summary conviction to a fine of three million dollars and to imprisonment for three years; and
- (b) on conviction on indictment to a fine of five million dollars and to imprisonment for five years.

(5) For the purposes of this section, “multiple electronic mail messages” means unsolicited data messages, including electronic mail and instant messages sent to more than fifty recipients within twenty-four hours.

Offences against the State.

18. (1) A person commits an offence if the person, whether in or out of Guyana, intentionally publishes, transmits or circulates by use of a computer system, a statement or words, either spoken or written, a text, video, image, sign, visible representation, or other thing, that —

- (a) advocates the use, without authority of law, of force as a means of accomplishing a governmental change within Guyana;

Cap. 8:01

(b) incites, counsels, urges, induces, aids or abets any person to commit, participate in the commission of, or to conspire with another person to commit treason under section 314 or 317 of the Criminal Law (Offences) Act;

(c) encourages, incites, induces, aids, abets, counsels any person to commit or to conspire with another person to commit any criminal offence against the President or any member of the Government;

Cap.10:11

(d) (i) encourages, entices, induces or motivates any person in or out of Guyana to join a terrorist group or to commit or participate in the commission of an offence of or in relation to terrorist financing under Part V of the Anti-Money Laundering and Countering the Financing of Terrorism Act; or

(ii) incites, urges, teaches or trains any person in or out of Guyana to commit or participate in the commission of a terrorist act or an offence under the Anti-terrorism and Terrorist Related Activities Act; or

No. 15 of 2015

(e) excites or attempts to excite ethnic divisions among the people of Guyana or hostility or ill-will against any person or class of persons on the ground of race.

(2) A person who commits an offence under subsection (1) shall be liable on conviction on indictment to imprisonment for five years.

(3) Where death of the President, any member of the Government or any other person occurs as a result of the commission of an offence under subsection (1), the person who commits the offence is liable on conviction on indictment to imprisonment for life.

(4) For the purposes of subsection (1), a statement or words, a text, video, image, sign, visible representation or other thing does not constitute an offence if it –

(a) expresses disapprobation of the measures of the Government

with a view to obtain their alteration by lawful means;

- (b) expresses disapprobation of the administrative or other action of the Government;
- (c) expresses that the President, any member of the Government or the Government has been misled or mistaken in their measures;
- (d) points out errors or defects of the Government, Constitution or Parliament; or
- (e) procures, by lawful means, the alteration of any matter of government.

Using a computer system to coerce, harass, intimidate, humiliate, etc. a person.

19. (1) A person commits an offence if the person, with intent to compel another person to do any act which the other person is not legally bound to do or to abstain from doing any act which the other person has a legal right to do, uses a computer system to publish or transmit electronic data that –

- (a) intimidates the other person; or
- (b) threatens the other person to use violence to him or a member of his family or injure his property or the property of his family.

(2) A person commits an offence if he uses a computer system –

- (a) to publish or transmit electronic data that is obscene, vulgar, profane, lewd, lascivious or indecent with intent to humiliate, harass or cause substantial emotional distress to another person; or
- (b) to repeatedly send to another person electronic data that is obscene, vulgar, profane, lewd, lascivious or indecent with intent to humiliate or harass the other person to the detriment of that person's health, emotional well-being, self-esteem or reputation.

(3) A person commits an offence if the person uses a computer system

to disseminate any information, statement or image, knowing the same to be false, that –

- (a) causes damage to the reputation of another person; or
- (b) subjects another person to public ridicule, contempt, hatred or embarrassment.

(4) A person who uses a computer system with the intent to extort a benefit from another person by threatening to publish electronic data containing personal or private information which can cause the other person public ridicule, contempt, hatred or embarrassment commits an offence.

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

- (a) on summary conviction to a fine of five million dollars and to imprisonment for three years; and
- (b) on conviction on indictment to a fine of ten million dollars and to imprisonment for five years.

(6) In subsection (1) –

(a) “intimidate” means –

- (i) to cause in the mind of a reasonable person an apprehension of injury to him or to any member of his family or to any of his dependants or of violence or damage to any person or property; or
- (ii) to cause a person substantial emotional distress; and
- (b) “injury” includes injury to a person in respect of his business, occupation, employment or other source of income, and includes an actionable wrong.

Infringement of
copyright, patents and
designs and
trademarks.
4&5 ELIZ. 2 Cap. 74

S.I. No. 79 of 1966

20. A person who uses a computer system to infringe –

- (a) the rights of the copyright owner under the Copyright Act 1956 as applied to Guyana with certain exceptions and modifications to form part of the law of Guyana by the Copyright (British Guiana) Order, 1966;
- (b) the rights of the proprietor of the patent or the rights of the

- Cap. 90:03 proprietor of a registered design under the Patents and Designs Act; or
- Cap. 90:01 (c) the rights of the proprietor of a registered trade mark under the Trade Marks Act,
- commits an offence and is liable on summary conviction to a fine of three million dollars and imprisonment for three years.

- Corporate liability. 21. (1) Where a body corporate commits an offence under this Act, the body corporate is liable to the fine applicable in respect of the offence.
- (2) Where a body corporate commits an offence under this Act and the court is satisfied that a director, manager, secretary, or other similar officer, of that body corporate-
- (a) consented or connived in the commission of the offence; or
- (b) failed to exercise due diligence to prevent the commission of the offence,
- that director, manager, secretary, or other similar officer commits an offence.
- (3) A person who commits an offence under subsection (2) is liable -
- (a) on summary conviction to a fine of five million dollars and to imprisonment for three years; and
- (b) on conviction on indictment to a fine of eight million dollars and to imprisonment for five years.

- Attempt, aiding or abetting. 22. A person who intentionally –
- (a) advises, incites, attempts, aids, abets, counsels, procures or facilitates the commission of any offence under this Act; or
- (b) conspires with another person to commit an offence under this Act,
- commits an offence and shall be punished for the offence as if he had committed the offence as a principal offender.

- Use of computer system to commit 23. Where an offence under any other law, not provided for in this Act,

A.D. 2018]

CYBERCRIME ACT 2018

[No. 16

offence under any other law.

is capable of being committed by a person through the use of a computer system, that other law shall be deemed to provide that the offence may be committed by a person through the use of a computer system and a person who commits the offence through the use of a computer system shall be liable to a fine of four times the monetary penalty provided by that law and to the same custodial sentence.

Offences prejudicing investigation.

24. (1) A person who knows or has reasonable grounds to believe that an investigation in relation to an offence under this Act is being or is about to be conducted, commits an offence if he intentionally -

- (a) makes a disclosure that is likely to prejudice the investigation; or
- (b) falsifies, conceals, destroys or otherwise disposes of, or causes or permits the falsification, concealment, destruction or disposal of, documents or electronic data that are relevant to the investigation.

(2) A person does not commit an offence under subsection (1)(a) if-

- (a) the person does not know or have reasonable grounds to believe that the disclosure is likely to prejudice the investigation;
- (b) the disclosure is made in the exercise of a function under this Act or in compliance with a requirement imposed under or by virtue of this Act;
- (c) the person is an attorney-at-law and the disclosure is -
 - (i) to a client in connection with the giving of legal advice to the client; or
 - (ii) to any person in connection with legal proceedings or contemplated legal proceedings,

but a disclosure does not fall within this paragraph if the disclosure is made with the intention of furthering a criminal purpose.

(3) A person does not commit an offence under subsection (1)(b) if the person –

- (a) does not know or suspect that the documents or electronic data are relevant to the investigation; or
- (b) does not intend to falsify, conceal, destroy or otherwise dispose of any facts disclosed by the documents or electronic data from any official carrying out the investigation.

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

- (a) on summary conviction to a fine of five million dollars and to imprisonment for three years; and
- (b) on conviction on indictment to a fine of eight million dollars and to imprisonment for five years.

PART III ENFORCEMENT

Service providers to store traffic data and subscriber information.

25. (1) Subject to subsection (2), a service provider shall store traffic data of subscribers for ninety days from the date on which the data is generated by a computer system.

(2) A Judge, if satisfied on an *ex parte* application by a police officer of the rank of Superintendent or above that traffic data is reasonably required for the purpose of a criminal investigation or criminal proceedings under this Act or any other law, may order a service provider to store traffic data of subscribers for a period of more than ninety days but not exceeding one year on a special case by case basis.

(3) The service provider shall keep subscriber information from the beginning of the service provision, and such information shall be kept for a period of ninety days after the service agreement has ended.

(4) A service provider who fails to comply with this section commits an offence and is liable on summary conviction to a fine of three million

dollars and to imprisonment for one year.

Extension of time for prosecution of an offence.

26. Notwithstanding the provisions of any written law prescribing the time within which proceedings for an offence punishable on summary conviction may be commenced, summary proceedings for an offence against this Act, or for attempting to commit, conspiring with another person to commit, or soliciting, inciting, aiding, abetting or counselling or causing or procuring the commission of, such an offence, or for attempting to solicit, incite, aid, abet, counsel or cause or procure the commission of such an offence, may be commenced within twelve months of the commission of the offence:

Provided that where an offence against this Act is punishable on summary conviction and on conviction on indictment, nothing in this section shall be deemed to restrict the power to commence, after the expiry of the aforesaid period of twelve months, proceedings for conviction on indictment for that offence or for any other act, relating to the offence, referred to in this section.

Jurisdiction.

27. (1) A court in Guyana shall have jurisdiction in respect of an offence under this Act where the act constituting the offence is carried out—

- (a) wholly or partly in Guyana;
- (b) by any person, whether in Guyana or elsewhere; or
- (c) by a person on board a vessel or aircraft registered in Guyana.

(2) For the purposes of subsection (1)(a), an act is carried out in Guyana if—

- (a) the person is in Guyana at the time when the act is committed;
- (b) the person is outside of Guyana at the time when the act is committed, but —
 - (i) a computer system located in Guyana or electronic

data on an electronic data storage medium located in Guyana is affected by, or contains information about, the act; or

- (ii) the transmission or effect of the act, or the damage resulting from the act, occurs, in whole or in part, within Guyana.

(3) Subject to subsection (1), a Magistrate's court has jurisdiction to hear and determine any offence under this Act, if—

- (a) the accused was within the magisterial district at the time when he committed the offence;
- (b) a computer system, containing any computer programme or electronic data which the accused used, was within the magisterial district at the time when the accused committed the offence; or
- (c) harm or damage occurred within the magisterial district, whether or not paragraph (a) or (b) applies.

Search and seizure.

28. (1) A Judge, if satisfied on an *ex parte* application by a police officer of the rank of Superintendent or above that there are reasonable grounds for suspecting that—

- (a) an offence under this Act has been or is about to be committed in any place; and
- (b) evidence that such an offence has been or is about to be committed is in that place,

may issue a warrant authorising a police officer, with such assistance as may be necessary, to enter the place to search for and seize the evidence, including any computer system, electronic data storage medium or electronic data.

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

- (a) the electronic data sought is stored in another computer system or electronic data storage medium; or

- (b) part of the electronic data sought is in another place within Guyana,

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

(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 electronic data storage medium;
- (b) inspect and check the operation of a computer system or electronic data storage medium;
- (c) make and retain a copy of electronic data;
- (d) remove electronic data from a computer system or render the computer system inaccessible;
- (e) take a printout of output of electronic data;
- (f) impound or similarly secure a computer system or part of it or an electronic data storage medium.

(4) A police officer who undertakes a search under this section shall secure any computer system or electronic data storage medium and maintain the integrity of the electronic data that is seized.

(5) The seizure of any evidence, including any computer system, electronic data storage medium or electronic data under this section shall be valid for a period of ninety days and may be extended for a further period of not more than one year by a Judge in Chambers.

(6) When the seizure is no longer necessary, or upon its expiry date, any computer system, electronic data storage medium or electronic data seized shall be immediately returned to the person to whom the warrant was addressed.

(7) Where a police officer in the execution of a warrant under this section decides to seize a computer system or an electronic data storage

medium, the police officer may, on the request of the person who is in possession or control of the computer system or electronic data storage medium, permit the person to make a copy of electronic data of the description and in the manner set out in subsection (8) from the computer system or electronic data storage medium.

(8) The electronic data shall –

- (a) to the satisfaction of the police officer be vital and of urgent need to the person before the expiry date referred to in subsection (6) and unrelated to the offence; and
- (b) be copied in the presence of the police officer onsite or at the place where the computer system is held in the custody of the police.

(9) For the purposes of this section seizure does not include the computer system or electronic data storage medium of a service provider unless the service provider is intentionally using his computer system to commit an offence under the Act.

Record of seized material.

29. (1) If a computer system or an electronic data storage medium is seized or rendered inaccessible in the execution of a warrant under section 28, the person who executed the warrant shall, at the time of the execution, 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 that list to –
 - (i) the person to whom the warrant is addressed; or
 - (ii) the occupier of the premises on which the warrant is executed.

(2) A person, who immediately before the execution of a warrant, had possession or control of a computer system or an electronic data storage medium seized, may request a copy of electronic data from the police officer who executed the warrant, and the police officer shall, as soon as is

reasonably practicable, comply with the request.

(3) Notwithstanding subsection (2), a police officer who seizes a computer system or an electronic data storage medium may refuse to provide a copy of electronic data if he has reasonable grounds for believing that providing a copy would-

- (a) constitute or facilitate the commission of 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 mentioned in subparagraph (i) or (ii).

Assistance.

30. (1) A person who has knowledge about the functioning of a computer system or an electronic data storage medium, or security measures applied to protect electronic data, that is the subject of a search warrant shall, if requested by the police officer authorised to undertake the search, assist the police officer by –

- (a) providing information that facilitates the undertaking of the search for and seizure of the computer system, electronic data storage medium or electronic data sought;
- (b) accessing and using the computer system or electronic data storage medium to search electronic data which is stored in, or lawfully accessible from or available to, that computer system or electronic data storage medium;
- (c) obtaining and copying electronic data; or
- (d) obtaining an intelligible output from a computer system or an electronic data storage medium in such a format that is admissible for the purpose of legal proceedings.

(2) A person who fails, without lawful excuse or justification, to comply with subsection (1) commits an offence and is liable on summary

conviction to a fine of three million dollars and to imprisonment for one year.

Production order.

31. A Judge, if satisfied on an *ex parte* application by a police officer of the rank of Superintendent or above that electronic data, traffic data, a printout or other information is reasonably required for the purpose of a criminal investigation or criminal proceedings under this Act or any other law, may order—

(a) a person in Guyana who is in possession or control of a computer system or an electronic data storage medium, to produce, from the computer system or electronic data storage medium, specified electronic data or a printout or other intelligible output of the electronic data; or

(b) a service provider in Guyana to produce traffic data relating to information transmitted from a subscriber through a computer system or from other relevant persons, or subscriber information about a person who uses the service,

and give it to a specified person within a specified period.

Expedited
preservation order.

32. (1) A Judge, if satisfied on an *ex parte* application by a police officer of the rank of Superintendent or above that there are reasonable grounds to believe that electronic data or traffic data that is reasonably required for the purpose of a criminal investigation, under this Act or any other law, is vulnerable to loss or modification, may make an order requiring a person in possession or control of electronic data or traffic data to preserve and maintain the integrity of the electronic data or traffic data for a period not exceeding ninety days.

(2) A Judge, on an *ex parte* application by a police officer of the rank of Superintendent or above, may order an extension of the period referred to in subsection (1) by a further specified period of ninety days or more but not exceeding one year on a special case by case basis.

Disclosure of traffic data order.

33. A Judge, if satisfied on an *ex parte* application by a police officer of the rank of Superintendent or above that there are reasonable grounds to believe that traffic data stored in a computer system or an electronic data storage medium is reasonably required for the purpose of a criminal investigation, under this Act or any other law, into a communication, may make an order requiring a person to disclose sufficient traffic data about the communication to identify –

- (a) the service provider; or
- (b) the path,

through which the communication was transmitted.

Confidentiality of order.

34. (1) A person who is the subject of an order under section 31, 32 or 33 shall keep confidential-

- (a) the fact that an order has been made;
- (b) the details of an order;
- (c) anything done pursuant to an order; or
- (d) any electronic data collected or recorded pursuant to an order.

(2) A person who intentionally and without lawful excuse or justification fails to comply with subsection (1) commits an offence and is liable on summary conviction to a fine of five million dollars and to imprisonment for three years.

Prohibition of disclosures.

35. (1) Except as provided in subsection (2), a person shall not disclose or deliver electronic data, traffic data or subscriber information or any other information acquired in the course of their duties under this Act to any other person.

(2) The provisions under subsection (1) shall not apply to any actions between a service provider and any other person permitted under any law, or performed for the benefit of investigating or prosecuting a person who has committed an offence under this Act.

(3) Any person who violates subsection (1) commits an offence and

shall be liable on summary conviction to a fine of five million dollars and to imprisonment for three years.

Protection of person
aiding in enforcement
of Act.

36. A person or service provider shall not be liable under a civil or criminal law for any actions taken or the disclosure of any electronic data or other information that may be disclosed pursuant to the enforcement of this Act.

Order for removal or
disablement of data.

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

Remote forensic tools.

38. (1) Where a Judge is satisfied on *ex parte* application by a police officer of the rank of Superintendent or above, that there are reasonable grounds to believe that electronic data which is required for the purpose of a criminal investigation into an offence under this Act or any other law, 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 utilise a remote forensic tool for the investigation.

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

- (a) the name, and if possible, the address, of the person who is suspected of committing the offence;
- (b) a description of the targeted computer system;
- (c) a description of the required tool, the extent and duration of its utilisation; and
- (d) reason for the use of the tool.

(3) Where an application is made under subsection (1), the Judge may

order that a person or a service provider support the installation of the remote forensic tool.

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

- (a) modifications to a computer system shall be limited to those that are necessary for the investigation;
- (b) modification to a computer system shall be undone, so far as possible, after the investigation; and
- (c) the police officer authorised under subsection (1) shall, as soon as possible thereafter, prepare a record of –
 - (i) the remote forensic tool 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 utilised under this section shall ensure that any information obtained by the utilisation of the remote forensic tool is protected against modification, unauthorised deletion and unauthorised access.

(6) An authorisation that is granted under this section shall cease to apply where -

- (a) the electronic data sought is collected;
- (b) there is no longer any reasonable ground for believing that the electronic data sought exists; or
- (c) the conditions of the authorisation are no longer present.

(7) For the purposes of this section, “remote forensic tool” means an investigative software or hardware installed on or attached to a computer system that is used to perform a task.

Order for payment of compensation.

39. (1) Where a person is convicted of an offence under this Act and the court 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 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 subsection (1) of its own motion or upon the application of a person who has suffered 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 in accordance with rules of court before sentence is passed on the person against whom the order is sought.

Forfeiture order.

40. (1) Subject to subsection (2), where a person is convicted of an offence under this Act, the court that heard the criminal case may, upon the application of the Director of Public Prosecutions, 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 State.

(2) Before making an order under subsection (1), the court shall give an opportunity to be heard to any person who—

- (a) claims to be the owner of the property; or
- (b) appears to the court to have an interest in the property.

(3) Where a person proves to the court that there is electronic data in a computer system or an electronic data storage medium forfeited which is useful to that person and unrelated to the offence committed, the Court shall make an order permitting the person to make a copy of that electronic data.

(4) Property forfeited to the State under subsection (1) shall vest in the State—

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

the forfeiture order; or

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

(5) Where property is forfeited to the State under this section, it shall be disposed of in such manner as the court orders.

Order for seizure and restraint regarding forfeiture.

41. Where an *ex parte* application is made by the Director of Public Prosecutions to a Judge and the Judge is satisfied that there are reasonable grounds to believe that there is in any building, place or vessel, any property in respect of which a forfeiture order under section 40 has been made, the Judge may issue—

- (a) a warrant authorising a police officer to search the building, place or vessel for that property and to seize –
- (i) that property if found; and
- (ii) any other property in respect of which the police officer believes, on reasonable grounds, that a forfeiture order under section 40 ought to have been 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.

Failure to comply with a court order.

42. If any person fails to comply with an order of the Court, the person commits an offence and shall be liable –

- (a) to a fine of one million dollars and to imprisonment for one year; and
- (b) a further daily fine for each day the offence continues, of not more than fifty thousand dollars until the relevant corrective action has been taken.

Evidence.

43. In any criminal proceeding under this Act or any other law –
- (a) any electronic data or traffic data, generated, retrieved or reproduced from a computer system or from an electronic data storage medium, and whether in electronic or printed form; or
 - (b) any computer system or electronic data storage medium, acquired in respect of any offence, shall be admissible as evidence.

Passed by the National Assembly on the 20th July, 2018.



S.E. Isaacs, A.A.,

Clerk of the National Assembly

(BILL No. 17/2016)