THE CYBERCRIMES ACT, 2015

(Act of 2015)

ARRANGEMENT OF SECTIONS

PART IV—*General*

A BILL

ENTITLED

AN ACT to Repeal and replace the Cybercrimes Act; and to provide for consequential 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 Jamaica, and by the authority of the same, as follows:—

PART I—*Preliminary*

Short title.

1. This Act may be cited as the Cybercrimes Act, 2015.

Interpretation.

2.—(1) In this Act—

"computer" means any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data and—

(a) includes any data storage facility or electronic communications system directly connected to or operating in conjunction with such device or group of such interconnected or related devices;

(b) does not include such devices as the Minister may prescribe by order published in the *Gazette;*

"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 any program or data;

"damage", for the purposes of sections 3(3), 4(4), 5(3), 6(5), 7(2), 8(2), 9(3) and 10(2), means any impairment to a computer, or to the integrity or availability of data, that—

(a) causes economic loss;

(b) modifies or impairs or potentially modifies or impairs the medical examination, diagnosis, treatment or care of one or more persons;

(c) causes or threatens physical injury or death to any person;

(d) threatens public health or public safety; or

(e) causes or threatens physical damage to a computer;

"data" includes—

(a) material in whatever form stored electronically;

(b) the whole or part of a computer program; and

(c) any representation of information or of concepts in a form suitable for use in a computer, including a program suitable to cause a computer to perform a function;

"electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities, and the word "electronically" shall be similarly construed;

"electronic communications system" means a system for creating, generating, sending, receiving, storing, displaying or otherwise processing electronic documents or data;

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

"key", in relation to any data or other computer output, includes any key, code, password, algorithm, authentication or authorization token, biometric identifier, gesture, or other data the use of which (with or without other keys)—

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

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

"output", in relation to a computer, data or program, means a statement or representation, whether in written, printed, pictorial, graphical, auditory, or other form—

(a) produced by a computer; or

(b) accurately translated from a statement or representation so produced;

"program" or "computer program" means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function, and a reference to a program includes any part of that program.

(2) For the purposes of this Act, a person obtains access to any program or data held in a computer if the person causes a computer to perform any function that—

(a) alters or erases the program or data;

(b) copies or moves the program or data to any storage medium other than that in which the program or data is held or to a different location in the storage medium in which the program or data is held;

(c) causes the program or data to be executed;

(d) is itself a function of the program or data; or

(e) causes the program or data to be output from the computer in which it is held, whether by having the program or data displayed or in any other manner,

and references to accessing, or to an intent to obtain access to, a computer shall be construed accordingly.

(3) For the purposes of subsection (2)(e)—

(a) a program is output if the data of which it consists is output, and it is immaterial whether the data is capable of being executed;

(b) in the case of data, it is immaterial whether the data is capable of being processed by a computer.

(4) For the purposes of this Act, a person who accesses, modifies, or uses, any program or data held in a computer, or causes the computer to perform any function, does so without authorisation if—

(a) he is not himself entitled to control the access, modification, use or function of the kind in question;

(b) he does not have consent for the access, modification, use or function of the kind in question from any person who is so entitled; and

(c) he is not acting pursuant to a power or function given to him under this Act or the Interception of Communications Act,

and the word "unauthorised" shall be construed accordingly.

(5) A reference in this Act to any "program or data held in a computer" includes a reference to any program or data held in any removable data storage medium which is for the time being in the computer.

(6) For the purposes of this Act, a modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer—

(a) any program or data held in the computer concerned is altered or erased;

(b) any program or data is added to the contents of the computer concerned; or

(c) any act occurs which impairs the normal operation of any computer,

and any act which contributes toward causing such a modification shall be regarded as causing it.

(7) A modification referred to in subsection (6) is unauthorised if—

(a) the person whose act causes the modification is not himself entitled to determine whether the modification should be made; and

(b) that person does not have consent for the modification from any person who is so entitled.

PART II—*Offences*

Unauthorised access to computer program or data.

3.—(1) A person who knowingly obtains, for himself or another person, any unauthorised access to any program or data held in a computer commits an offence.

(2) The intent required for the commission of an offence under subsection (1) need not be directed at—

(a) any specifically identifiable program or data;

(b) a program or data of any specifically identifiable kind; or

(c) a program or data held in any specifically identifiable computer.

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

(a) summary conviction before a Resident Magistrate to—

(i) in the case of a first offence, a fine not exceeding three million dollars or imprisonment for a term not exceeding three years;

(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;

(b) conviction on indictment before a Circuit Court to—

(i) in the case of a first offence, a fine or imprisonment for a term not exceeding seven years;

(ii) if any damage is caused as a result of the commission of the offence, a fine or imprisonment for a term not exceeding ten years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding fifteen years.

Access with intent to commit or facilitate commission of offence.

4.—(1) A person commits an offence if that person accesses any program or data held in a computer with the intent to—

(a) commit any offence punishable by imprisonment for a term that exceeds one year; or

(b) facilitate the commission of an offence referred to in paragraph (a), whether by himself or by any other person.

(2) A person may commit an offence under subsection (1) even if the facts are such that the commission of the offence referred to in subsection (1)(a) is impossible.

(3) For the purposes of this section, it is immaterial whether—

(a) the access referred to in subsection (1) is with or without authorisation;

(b) the offence referred to in subsection (1)(a) is committed at the same time when the access is secured or at any other time.

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

(a) summary conviction before a Resident Magistrate to—

(i) in the case of a first offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years;

(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;

(b) conviction on indictment before a Circuit Court to—

(i) in the case of a first offence, a fine or imprisonment for a term not exceeding seven years;

(ii) if any damage is caused as a result of the commission of the offence, a fine or imprisonment for a term not exceeding ten years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding fifteen years.

Unauthorised modification of computer program or data.

5.—(1) A person who does any act which that person knows is likely to cause any unauthorised modification of the contents of any computer, commits an offence.

(2) For the purposes of subsection (1)—

(a) the act in question need not be directed at—

(i) any specifically identifiable program or data or type of program or data;

(ii) any program or data held in a specifically identifiable computer; and

(b) it is immaterial whether the modification is, or is intended to be, permanent or temporary.

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

(a) summary conviction before a Resident Magistrate to—

(i) in the case of a first offence, a fine not exceeding three million dollars or imprisonment for a term not exceeding three years;

(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;

(b) conviction on indictment before a Circuit Court to—

(i) in the case of a first offence, a fine or imprisonment for a term not exceeding seven years;

(ii) if any damage is caused as a result of the commission of the offence, a fine or imprisonment for a term not exceeding ten years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding fifteen years.

Unauthorised interception of computer function or service.

6.—(1) A person commits an offence if that person knowingly—

(a) secures unauthorised access to any computer for the purpose of obtaining, directly or indirectly, any computer service; or

(b) without authorisation, directly or indirectly intercepts or causes to be intercepted any function of a computer.

(2) For the purposes of subsection (1), the access or interception referred to need not be directed at—

(a) any specifically identifiable program or data or type of program or data; or

(b) any program or data held in a specifically identifiable computer.

(3) Subsection (1) shall not apply to any interception permitted under the provisions of the *Interception of Communications Act*.

(4) For the purposes of this section, intercepting includes listening to or viewing, by use of technical means, or recording, a function of a computer or acquiring the substance, meaning or purport of any such function.

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

(a) summary conviction before a Resident Magistrate to—

(i) in the case of a first offence, a fine not exceeding three million dollars or imprisonment for a term not exceeding three years;

(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;

(b) conviction on indictment before a Circuit Court, to—

(i) in the case of a first offence, a fine or imprisonment for a term not exceeding seven years;

(ii) if any damage is caused as a result of the commission of the offence, a fine or imprisonment for a term not exceeding ten years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding fifteen years.

Unauthorised obstruction of operation of computer.

7.—(1) A person commits an offence if that person, without authorisation or without lawful justification or excuse, wilfully causes, directly or indirectly—

(a) a degradation, failure, interruption or obstruction of the operation of a computer; or

(b) a denial of access to, or impairment of, any program or data stored in a computer.

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

(a) summary conviction before a Resident Magistrate, to—

(i) in the case of a first offence, a fine not exceeding three million dollars or to imprisonment for a term not exceeding three years; or

(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;

(b) conviction on indictment before a Circuit Court, to—

(i) in the case of a first offence, a fine or imprisonment for a term not exceeding seven years; or

(ii) if any damage is caused as a result of the commission of the offence, a fine or imprisonment for a term not exceeding ten years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding fifteen years.

Computer related fraud or forgery.

8.—(1) A person commits an offence if that person fraudulently, with intent to procure an advantage for himself or another person—

(a) causes loss of property to another person by any—

(i) input, alteration, deletion or suppression of data; or

(ii) interference with any function of a computer; or

(b) accesses any computer and inputs, alters, deletes or suppresses any data ("the original data") with the intention that the data, after such input, alteration, deletion or suppression (whether or not that data is readable or intelligible), be considered or acted upon as if that data were the original data.

(2) A person who commits an offence under subsection (1) shall be liable upon—

(a) summary conviction before a Resident Magistrate, to—

(i) in the case of a first offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years;

(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;

(b) conviction on indictment before a Circuit Court, to—

(i) in the case of a first offence, a fine or imprisonment for a term not exceeding ten years;

(ii) if any damage is caused as a result of the commission of the offence, a fine or imprisonment for a term not exceeding fifteen years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding twenty years.

Use of computer for malicious communication.

9.—(1) A person commits an offence if that person uses a computer to send to another person any data (whether in the form of a message or otherwise)—

(a) that is obscene, constitutes a threat or is menacing in nature; and

(b) with the intention to harass any person or cause harm, or the apprehension of harm, to any person or property,

but (for the avoidance of doubt) nothing in this section shall be construed as applying to any communication relating to industrial action, in the course of an industrial dispute, within the meaning of the Labour Relations and Industrial Disputes Act.

(2) An offence is committed under subsection (1) regardless of whether the actual recipient of the data is or is not the person to whom the offender intended the data to be sent.

(3) A person who commits an offence under subsection (1) shall be liable upon—

(a) summary conviction before a Resident Magistrate, to—

(i) in the case of a first offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years;

(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;

(b) conviction on indictment before a Circuit Court, to—

(i) in the case of a first offence, a fine or imprisonment for a term not exceeding ten years;

(ii) if any damage is caused as a result of the commission of the offence, a fine or imprisonment for a term not exceeding fifteen years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding twenty years.

Unlawfully making available devices or data for commission of offence.

10.—(1) A person commits an offence who, for the purpose of committing, or facilitating the commission of, an offence under any of sections 3 to 9, possesses, receives, manufactures, sells, imports, distributes, discloses or otherwise makes available—

(a) a computer;

(b) any key; or

(c) any other data or device,

designed or adapted primarily for the purpose of committing an offence under any of sections 3 to 9.

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

(a) summary conviction before a Resident Magistrate, to—

(i) in the case of a first offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years;

(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;

(b) conviction before a Circuit Court to—

(i) in the case of a first offence, a fine or imprisonment for a term not exceeding ten years;

(ii) if any damage is caused as a result of the commission of the offence, a fine or imprisonment for a term not exceeding fifteen years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding twenty years.

Offences relating to protected computers.

11.—(1) Where a computer in respect of which an offence under any of sections 3 to 10 is committed is a protected computer, the offender shall be tried on indictment in the Circuit Court and shall be liable upon conviction to a fine or imprisonment for a term not exceeding twenty-five years.

(2) For the purposes of subsection (1), "protected computer" means a computer which, at the time of the commission of the offence, the offender knows, or ought reasonably to know, is necessary for, or used directly in connection with—

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

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

(c) confidential educational material, such as examination materials;

(d) 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, toll roads, traffic lights, bridges, airports and seaports; or

(e) the protection of public safety, including systems related to essential emergency services such as police, fire brigade services, civil defence and medical services.

(3) The Minister may, by order published in the *Gazette* and subject to affirmative resolution, amend subsection (2) so as to add, vary or exclude any use.

Inciting, *etc.*

12. A person who intentionally incites, attempts, aids or abets the commission of any offence under any of sections 3 to 10 ("the substantive offence"), or conspires with another person to commit the substantive offence, commits an offence and shall be liable to the same penalty as applies to the substantive offence, and to be proceeded against and punished accordingly.

Offences prejudicing investigation

13.—(1) This section applies if a person knows or has reasonable grounds to believe that an investigation in relation to an offence under this Part is being, or is about to be, conducted.

(2) The person commits an offence if the person—

(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 data that are relevant to the investigation.

(3) A person does not commit an offence under subsection (2)(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; or

(c) the person is an attorney-at-law and the disclosure falls within subsection (4).

(4) A disclosure falls within this subsection if it is a disclosure—

(a) to, or to a representative of, a client of the attorney-at-law in connection with the giving by the attorney-at-law of legal advice to the client; or

(b) to any person in connection with legal proceedings or contemplated legal proceedings,

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

(5) A person does not commit an offence under subsection (2)(b) if the person—

(a) does not know or suspect that the documents are relevant to the investigation; or

(b) does not intend to conceal any facts disclosed by the documents from any official carrying out the investigation.

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

(a) on conviction before a Resident Magistrate, to a fine not exceeding three million dollars or imprisonment for a term not exceeding three years; or

(b) on conviction on indictment before a Circuit Court, to a fine or imprisonment for a term not exceeding ten years.

Offences by bodies corporate.

14.—(1) For the avoidance of doubt, where a body corporate commits an offence under this Act, the body corporate shall be 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) connived in the commission of the offence, that director, manager, secretary, or other similar officer, shall also be liable to be proceeded against for the offence and punished accordingly; or

(b) failed to exercise due diligence to prevent the commission of the offence, that director, manager, secretary, or other similar officer, shall be liable—

(i) on conviction before a Resident Magistrate, to a fine not exceeding two million dollars or imprisonment for a term not exceeding two years; or

(ii) on conviction on indictment before a Circuit Court to a fine or imprisonment for a term not exceeding six years.

Compensation.

15.—(1) Where a person is convicted of an offence under this Part, the court may, in the same proceedings and in addition to any penalty imposed under this Part, order the person convicted to pay a fixed sum as compensation to any person who has suffered loss as a result of the commission of the offence.

(2) An order under subsection (1) shall be without prejudice to any other cause of action which the person who has suffered loss 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 any person in accordance with subsection (4).

(4) A person who has suffered loss as a result of the commission of an offence under this Part may apply in accordance with rules of court for an order under subsection (1), at any time before sentence is passed on the person against whom the order is sought.

PART III—*Investigations*

Interpretation and scope of Part III.

16.—(1) In this Part—

(a) "computer material" includes—

(i) data;

(ii)a computer (computer A) or any part thereof;

(iii) any other computer (computer B) or any part thereof, if—

(A) data from computer A is available to computer B, or data from computer B is available to computer A; and

(B) there are reasonable grounds for believing that such data is stored in computer B; and

(iv) any data storage medium;

(b) the power to seize includes the power to—

(i) make and retain a copy of data, including by using on-site equipment;

(ii) render inaccessible, or remove, data in a computer; and

(iii) take a printout of, or otherwise reproduce or capture, the output of any computer or data.

(2) This Part shall apply for the purpose of investigations and enforcement proceedings in respect of offences under any law.

Preservation of data.

17.—(1) Where a constable is satisfied that—

(a) data stored in a computer or any data storage medium is reasonably required for the purposes of a criminal investigation; and

(b) there are reasonable grounds for suspecting that the data may be destroyed or rendered inaccessible,

the constable may, by notice in accordance with subsection (2) given to the person in possession or control of the computer or data storage medium (as the case may be), require the person to ensure that the data be preserved.

(2) The notice referred to in subsection (1) shall be in writing and shall specify—

(a) the name of the person in possession or control of the computer or data storage medium (as the case may be) or the address where the computer or data storage medium (as the case may be) is located;

(b) the period for which the data is required to be preserved, being a period not exceeding sixty days; and

(c) the requirements to be complied with for the preservation of the data.

(3) For the purposes of subsection (2), "address" includes a location, e-mail address, telephone number or other number or designation used for the purpose of identifying a computer or electronic communications system.

(4) The period specified under subsection (2), or in any previous order made under this subsection, may be extended, upon the order of a Resident Magistrate on an application without notice, for such further period as may be specified by the Resident Magistrate in the order.

(5) A person commits an offence if the person fails, without reasonable excuse, to comply with a requirement imposed on that person by a notice or order under this section.

(6) A person commits an offence if, in purported compliance with a requirement imposed on that person under a notice or order made under this section, the person—

(a) makes a statement that the person knows to be false or misleading in a material particular; or

(b) recklessly makes a statement that is false or misleading in a material particular.

(7) A person who commits an offence under subsection (5) or (6) is liable—

(a) upon conviction before a Resident Magistrate, to a fine not exceeding three million dollars or imprisonment for a term not exceeding three years;

(b) upon conviction on indictment before a Circuit Court, to a fine or imprisonment for a term not exceeding seven years.

Search and seizure warrants.

18.—(1) A Resident Magistrate may issue a warrant under this subsection, if satisfied by information on oath that there are reasonable grounds to suspect that there may be in any place any computer material that—

(a) may be relevant as evidence in proving an offence; or

(b) has been acquired by a person for, or in, the commission of an offence or as a result of the commission of an offence.

(2) A warrant under subsection (1) shall authorise a constable, with such assistance as may be necessary, to enter the place specified in the warrant to search for and seize the computer material.

Record of seized material.

19.—(1) If any computer material is seized or rendered inaccessible in the execution of a warrant under section 18(1), the person who executed the warrant shall, during the execution, or as soon as possible thereafter—

(a) make a list of what has been seized or rendered inaccessible; 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) A person who, immediately before the execution of a warrant, had possession or control of data seized in the execution, may request a copy of the data from the constable who executed the warrant, and the constable shall, as soon as is reasonably practicable, comply with the request if the conditions under subsection (3) are satisfied.

(3) The conditions referred to in subsection (2) are that providing the copy would not—

(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 sub-paragraph (i) or (ii).

(4) A person who executes a warrant under section 18(1) shall take all reasonable steps to preserve the computer material seized or rendered inaccessible.

(5) A person who contravenes subsection (4) commits an offence and is liable upon conviction before a Resident Magistrate, to a fine not exceeding Three Million Dollars, or in default of payment thereof to a term of impresonment not exceeding three (3) years.

(6) Where computer material is seized or rendered inaccessible in the execution of a warrant under section 18(10, a person commits an offence if that person—

(a) uses the data comprised in the computer material for any purpose otherwise than in accordance with this Act; or

(b) discloses such data other than for the purposes of this Act, and is liable upon conviction before a Resident Magistrate to a fine not exceeding three million dollars or, in default of payment thereof, to a term of imprisonment not exceeding three years.

Forfeiture.

20.—(1) Where any computer material is seized pursuant to section 19, an order under subsection (2) or (4) may be made in respect of the computer material.

(2) Where—

(a) any person is convicted of an offence; and

(b) the court concerned is satisfied that—

(i) the person owns computer material used in the commission of the offence;

(ii) the owner of computer material permitted it to be used in the commission of the offence; or

(iii) the circumstances are otherwise such that it is just to do so,

the court shall, upon the application of the Director of Public Prosecutions, order the forfeiture of the computer material used in the commission of the offence.

(3) On the application of the Director of Public Prosecutions before a Resident Magistrate's Court having jurisdiction in the area where the computer material is seized, or a Judge of the Supreme Court in Chambers, the Court or Judge may make an order in accordance with subsection (4) notwithstanding that the conditions mentioned in subsection (2) have not been satisfied.

(4) Where an application is made under subsection (3), the Court or Judge (as the case may be) may order the forfeiture of the computer material if the Court or Judge is satisfied that—

(a) the computer material has been abandoned; or

(b) the circumstances in which the computer material was seized give reasonable cause to suspect that it was being used or has been used for committing an offence under this Act,

and it is otherwise just to do so.

(5) Where the Director of Public Prosecutions intends to apply for an order under subsection (4), the Director of Public Prosecutions shall give to any person who, to the knowledge of the Director of Public Prosecutions was at the time of the seizure, the owner of the computer material, notice of the seizure and the intention to apply for a forfeiture order and the grounds therefor.

(6) Where the Director of Public Prosecutions is unable to ascertain the owner of, or any person having an interest in, any computer material to which this section applies, the Director of Public Prosecutions shall publish a notice in a daily newspaper in circulation throughout Jamaica, of the intention to apply for a forfeiture order, not less than thirty days prior to the application.

(7) Any person having a claim to any computer material seized under this Act may appear at the hearing of the application for forfeiture and show cause why such an order should not be made.

(8) Where, on the hearing of an application for forfeiture under subsection (3), no person appears before the Judge to show cause as mentioned in subsection (7), the computer material shall be presumed to have been abandoned.

(9) If, upon the application of a person prejudiced by an order made under subsection (2) or (4), the Court or Judge (as the case may be) is satisfied that it is just in the circumstances of the case to revoke or vary the order, the Court or Judge may—

(a) revoke or vary the order upon such terms and conditions, if any, as the Court or Judge considers appropriate; and

(b) without prejudice to the generality of paragraph (a), require the person to pay in respect of the storage, maintenance, administrative expenses, security and insurance of the

computer material, such amount as may be charged or borne by the person in whose custody the computer material was kept.

(10) An application under subsection (9) shall be made within thirty days after the date of the forfeiture order or within such longer period, not exceeding six months from the date of the order, as the Court or Judge (as the case may be) may allow.

Production orders.

21.—(1) A Resident Magistrate, if satisfied on the basis of an application made by a constable, that any data or other computer output specified in the application is reasonably required for the purpose of a criminal investigation or criminal proceedings, may make an order under subsection (2).

(2) An order under this subsection may require a person in possession or control of the data or other computer output to produce it in intelligible form to the constable.

(3) Where a production order requires the person to whom it is addressed to produce any data or other computer output in intelligible form, that person—

(a) shall be entitled to use any key in his possession or control to obtain access to the data or output;

(b) shall be taken to have produced the data or output in intelligible form if—

(i) the person makes, instead, a disclosure of any key to the data or output; and

(ii) the data or output is produced in accordance with the order, with respect to the person to whom, and the time in which, the person was ordered to produce the data or output.

(4) Where a constable has reasonable grounds to believe that—

(a) a key to any data or other computer output is in the possession of any person; and

(b) the production of the key is necessary for the purposes of the investigation in relation to which—

(i) the constable makes, or intends to make, an application for a production order; or

(ii) a production order has been issued to the constable,

the constable may apply to the Resident Magistrate for such ancillary order, as may be required in the circumstances, to be included in the production order.

(5) An application under subsection (4) may be made—

(a) in any case referred to in subsection (4)(b)(i), at the time of the application for the production order;

(b) in any case referred to in subsection (4)(b)(ii), at any time after the making of the production order.

(6) Where the Resident Magistrate grants an application under subsection (4), the Resident Magistrate shall—

(a) in the case of an application under subsection (5)(a), include the ancillary order in the production order;

(b) in the case of an application made under subsection (5)(b), vary the production order to include the ancillary order.

(7) The ancillary order shall—

(a) describe the data or other computer output to which it relates;

(b) specify the time by which the order is to be complied with, being a reasonable time in all the circumstances; and

(c) set out the production that is required by the order and the form and manner in which the production is to be made,

and any such order may require the person to whom it is addressed to keep secret the contents and existence of the order.

(8) In granting an ancillary order, the Resident Magistrate shall—

(a) take into account—

(i) the extent and nature of any other information, in addition to the data or computer output in question, to which the key is also a key;

(ii) any adverse effect that complying with the order might have on any lawful business carried on by the person to whom the order is addressed; and

(b) require only such production as is proportionate to what is sought to be achieved, allowing, where appropriate, for production in such manner as would result in the putting of the information in intelligible form other than by disclosure of the key itself.

(9) An ancillary order shall not require—

(a) the production of any key which—

(i) is intended to be used for the purpose only of generating electronic signatures; and

(ii) has not in fact been used for any other purpose; or

(b) the production of any data or other computer output to a person other than the constable or such other person as may be specified in the order.

(10) Where an ancillary order is addressed to a person who—

(a) is not in possession or control of the data or other computer output to which the order relates; or

(b) is incapable, without the use of a key that is not in the person's possession or control, of obtaining access to the data or other computer output or producing it in intelligible form,

the person shall be taken to have complied with the order if the person produces any key to the data or other computer output (as the case may be), that is in the person's possession.

(11) It shall be sufficient for the purpose of complying with an ancillary order for the person to whom it is addressed to produce only those keys the production of which is sufficient to enable the person to whom they are produced to obtain access to the data or other computer output concerned and to put it into intelligible form.

(12) Where—

(a) the production required by an ancillary order allows the person to whom it is addressed to comply with the order without producing all of the keys in the person's possession or control; and

(b) there are different keys or combinations of keys in the possession or control of that person the production of which would constitute compliance with the order,

the person may select which of the keys, or combination of keys, to produce for the purpose of complying with the order.

(13) Where an ancillary order is addressed to a person who—

(a) was in possession or control of the key but is no longer in possession or control of it;

(b) if the person had continued to have possession or control of the key, would be required by virtue of the order to produce it; and

(c) is in possession or control of information that would facilitate the obtaining or discovery of the key or the putting of the data or other computer output concerned into intelligible form,

that person shall produce to the person to whom that person would have been required to produce the key, all such information as is mentioned in paragraph (c).

(14) A constable who obtains an ancillary order shall ensure that such arrangements are made as are necessary for securing that—

(a) a key produced in pursuance of the order is used to obtain access to, or put into intelligible form, only data or other computer output in relation to which the order was made;

(b) every key produced in pursuance of the order is stored, for so long as it is retained, in a secure manner, and any records of such key are destroyed as soon as no longer needed to access the data or other computer output concerned or put it into intelligible form; and

(c) the number of—

(i) persons to whom the key is produced or otherwise made available; and

(ii) copies made of the key,

is limited to the minimum that is necessary for the purpose of enabling the data or other computer output concerned to be accessed or put into intelligible form.

(15) A constable who knowingly contravenes subsection (14) commits an offence and, upon conviction before a Resident Magistrate, is liable to a fine not exceeding one million dollars or imprisonment for a term not exceeding one year, or both such fine and imprisonment.

(16) A person commits an offence if the person fails, without reasonable excuse, to comply with a requirement imposed on that person by an order made under this section.

(17) A person who commits an offence under subsection (16) is liable—

(a) upon conviction before a Resident Magistrate, to a fine not exceeding four million dollars or imprisonment for a term not exceeding four years;

(b) upon conviction on indictment before a Circuit Court, to a fine or imprisonment for a term not exceeding seven years.

(18) In this section—

"electronic signature" means anything in electronic form that—

(a) is incorporated into, or otherwise logically associated with, any electronic information;

(b) is generated by the signatory or other source of the information; and

(c) is used for the purpose of facilitating, by means of a link between the signatory or other source of the information, the establishment of the authenticity of the information, the establishment of its integrity, or both;

"information" includes data, text, images, sounds, codes, computer programs, software and databases.

PART IV—*General*

Jurisdiction.

22.—(1) This Act applies in res pect of conduct occurring—

(a) wholly or partly in Jamaica;

(b) wholly or partly on board a Jamaican ship or Jamaican aircraft;

(c) wholly outside of Jamaica and attributable to a Jamaican national; or

(d) wholly outside of Jamaica, if the conduct affects a computer or data—

(i) wholly or partly in Jamaica; or

(ii) wholly or partly on board a Jamaican ship or Jamaican aircraft.

(2) In this section—

"Jamaican aircraft" has the meaning assigned to it by section 2 of the *Civil Aviation Act*;

"Jamaican national" means a person who—

(a) is a citizen of Jamaica;

(b) has a connection with Jamaica of a kind which entitles that person to be regarded as belonging to, or as being a native or resident of, Jamaica for the purposes of the laws of Jamaica relating to immigration; or

(c) is a company or other legal entity constituted in Jamaica in accordance with the laws of Jamaica;

"Jamaican ship" has the meaning assigned to it by section 2 of the *Shipping Act*.

Regulations.

23.—(1) The Minister may make regulations in order to give effect to the purposes of this Act.

(2) Notwithstanding section 29(b) of the *Interpretation Act,* and subject to affirmative resolution, regulations made under this Act may provide for penalties up to a maximum of one million dollars, on summary conviction or conviction on indictment for contravention of the regulations.

Power to amend monetary penalties by order.

24. The Minister may, by order subject to affirmative resolution and published in the *Gazette*, amend any monetary penalty imposed by this Act or the maximum monetary penalty specified in section 23(2).

Review of Act after three years.

25. The provisions of this Act shall be reviewed by a Joint Select Committee of the Houses of Parliament after the expiration of three years from the date of commencement of this Act.

Repeal of *Cybercrimes Act*, 2010.

26. The *Cybercrimes Act, 2010*, is hereby repealed.

Validity of proceedings not affected by repeal.

27. The validity of any proceedings taken, or any order in force under the *Cybercrimes Act, 2010*, immediately before the date of commencement of this Act, shall not be affected by the repeal of that Act, and any such proceedings shall be continued and determined, and any such order shall continue in force for such duration, as if such repeal had not been made.

Amendment of *Interception of Communications Act.*

28. The *Interception of Communications Act* is amended, in section 2, in the definition of "key", by deleting the words "means any key, code, password, algorithm" and substituting therefor the words "includes any key, code, password, algorithm, authentication or authorization token, biometric identifier, gesture,".

Passed in the House of Representatives this 13th day of October, 2015 with two (2) amendments.

MICHAEL A. PEART
Speaker.

Passed in the Senate this 27th day of November, 2015 with seventeen (17) amendments.

NORMAN W. GRANT
Acting President.

MEMORANDUM OF OBJECTS AND REASONS

A decision has been taken to repeal the Cybercrimes Act, 2010, and replace it with a new Cybercrimes Act which incorporates the amendments recommended by the Joint Select Committee of the Houses of Parliament pursuant to a review conducted under section 21 of the Cybercrimes Act, 2010.

This Bill seeks to give effect to that decision.

New offences provided for in the Bill include—

(a) computer related fraud or forgery;

(b) use of computers for malicious communications; and

(c) unauthorised disclosure of investigations (tipping-off).

Provision for forfeiture of computer material used in the commission of an offence is also included in the Bill.

PHILLIP PAULWELL

Minister of Science, Technology, Energy and Mining

A BILL

ENTITLED

AN ACT to Repeal and replace the Cybercrimes Act.

As passed in the Honourable House of Representatives.

As passed in the Honourable Senate.

PRINTED BY JAMAICA PRINTING SERVICES (1992) LTD.,
(GOVERNMENT PRINTERS), DUKE STREET, KINGSTON, JAMAICA.