ELECTRONIC CRIMES BILL, 2013

EXPLANATORY NOTES

This Bill contains 4 Parts and seeks to provide for the prevention and punishment of electronic crimes.

PART I of the Bill, *Clauses 1-4*, deals with matters of a preliminary nature. *Clause 1* is the standard citation and commencement provision.

Clause 2 sets out the interpretation of terms used in the Bill such as "access", "contaminant", "data", "damage", "function", "traffic data, which have been defined to ensure that the intended purpose of the legislation is achieved.

Clause 3 sets out the application of the Bill. *Clause 4* provides that the State is bound by the provisions of the Bill.

PART II of the Bill, *Clauses 5 -20*, creates 16 offences: access and interference, sending offensive messages through communication service, etc, identity theft, electronic defamation, electronic forgery, electronic fraud, malicious code, violation of privacy, misuse of encryption, child pornography, sensitive electronic system, electronic terrorism, prank calls to law enforcement, electronic stalking, spoofing and unauthorized access to code.

PART III of the Bill, *Clauses 21 – 30* provides for investigations and procedures of electronic crimes.

In that connection, this Part *Clauses 21 – 23* makes provision for the grant of a preservation order, disclosure of preserved data order and production order by a Judge upon application in Chambers by a police officer of the rank of Inspector. *Clause 24* makes provision for a police officer to apply to a Judge in Chambers for the issue of a warrant that enables the police officer to enter any premises to access, search and seize any data, program or information for the purposes of a criminal investigation. *Clause 25* provides for a police officer to collect or record any traffic data in real time.

Clause 26 provides that a mobile phone service provider shall provide mobile phone tracking to the law enforcement agencies upon request in cases of emergencies. *Clause 27* makes provision for a police officer to arrest without warrant a person reasonably suspected of committing an offence under the Act.

Clause 28 provides for the del**e**tion of indecent photographs of children. *Clause 29* sets out the exceptions where a person should not use or disclose data obtained. *Clause 30* provides that a service provider will not be liable for any actions taken or any information provided or disclosed to law enforcement agencies.

PART IV of the Bill, *Clauses 31 - 35* deals with matters of a miscellaneous nature and in that connection it makes provision for the institution of criminal proceedings, extraditable offences, order for compensation, forfeiture and for the making of Regulations.

.....
A.K. CAJETON HOOD
Hon. Attorney General

ELECTRONIC CRIMES BILL, 2013

GRENADA

ACT NO. OF 2013

ARRANGEMENT OF CLAUSES

PART I
PRELIMINARY

PART II
OFFENCES

PART III
INVESTIGATIONS AND PROCEDURES

PART IV
MISCELLANEOUS

ELECTRONIC CRIMES BILL, 2013

GRENADA

ACT NO. OF 2013

AN ACT to provide for the prevention and punishment of electronic crimes and for related matters.

BE IT ENACTED by the Queen's Most Excellent Majesty, by and with the advice and consent of the Senate and House of Representatives of Grenada, and by the authority of the same as follows –

PART I
PRELIMINARY

Short title and commencement

1. (1) This Act may be cited as the-

ELECTRONIC CRIMES ACT, 2013

(2) This Act shall come into force on a day to be fixed by the Minister by Order published in the *Gazette*.

Interpretation

2. In this Act-

"access" in the context of an electronic system means to communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of the electronic system;

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

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

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

"contaminant" means a set of electronic instructions that are designed–

(a) to modify, destroy, record, transmit data or program residing within an electronic system; or

(b) by any means to usurp the normal operation of an electronic system or electronic network;

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

“data” includes representations of facts, information or concepts that are being prepared or have been prepared in a form suitable for use in an electronic system including electronic program, text, images, sound, video and information within a database or electronic system;

“decryption” means the process of transforming or unscrambling encrypted data from its unreadable and incomprehensible format to its plain version;

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

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

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

“electronic system” means an electronic device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data and includes an electronic storage medium;

“encryption” means the process whereby data is transformed or scrambled from its plain version to an unreadable or incomprehensible format, regardless of the technique utilized for such transformation or scrambling and irrespective of the medium in which such data occurs or can be found for the purposes of protecting such data;

“function” includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within an electronic system;

“malicious code” means an electronic program or a hidden function in a program that infects data with or without attaching its copy to a file and

is capable of spreading over an electronic system with or without human intervention including virus, worm or Trojan horse;

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

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

"service provider" means–

(a) a person who provides an information and communication service including the sending, receiving, storing or processing of the electronic communication or the provision of other services in relation to it through an electronic system;

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

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

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

"subscriber" means a person listed as using the services of a service provider;

"subscriber information" means any information contained in any form that is held by a service provider, relating to subscribers of its services other than traffic data and by which can be established–

(a) the type of communication service used, the technical provisions taken thereto and the period of service;

(b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; or

(c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement;

"traffic data" means any data relating to a communication by means of an electronic system, generated by an electronic system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service; and

"unauthorized access" means access of any kind by a person to an electronic system or data held in an electronic system which is unauthorized or done without authority or is in excess of authority, if the person is not himself entitled to control access of the kind in question to the electronic system or data and the person does not have consent to such access from a person so entitled.

Application

3. This Act applies where–

(a) an offence under this Act was committed in Grenada;

(b) any act of preparation towards an offence under this Act or any part of the offence was committed in Grenada or where any result of the offence has had an effect in Grenada;

(c) an offence under this Act was committed by a Grenadian national or a person resident or carrying out business in Grenada or visiting Grenada or staying in transit in Grenada;

(d) an offence under this Act was committed in relation to or connected with an electronic system or data in Grenada or capable of being connected, sent to, used by or with an electronic system in Grenada; or

(e) an offence under this Act was committed by any person, of any nationality or citizenship or in any place outside or inside Grenada, having an effect on the security of Grenada or its nationals, or having universal application under international law, custom and usage.

Act binding on State

4. This Act binds the State.

PART II
OFFENCES

Unauthorised access and interference

5. (1) A person shall not knowingly or without lawful excuse or justification, or without permission of the owner or any other person who is in charge of an

electronic system or network–

(a) gain access or secure to such electronic system or network;

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

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

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

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

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

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

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

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

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

(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding two hundred thousand dollars or to a term of imprisonment not exceeding three years, or to both.

Sending offensive messages through communication services, etc

6. (1) A person shall not knowingly or without lawful excuse or justification send by means of an electronic system or an electronic device–

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

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

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

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

(3) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding one hundred thousand dollars or to a term of imprisonment not exceeding one year or to both.

Identity theft

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

(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding fifty thousand dollars or to a term of imprisonment not exceeding three years or to both.

Electronic forgery

8. (1) A person shall not knowingly or without lawful excuse or justification, interfere with data or an electronic system so that he, she, or another person uses the data or the electronic system to induce a person to accept it as genuine and by reason of so accepting it to do or not to do any act to his or her own or any other person's prejudice or injury.

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

Electronic fraud

9. (1) A person shall not knowingly or without lawful excuse or justification gain, interfere with data or an electronic system –

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

(b) with intent to deceive another person; or

(c) with intent to defraud a person,

where such an act is likely to cause damage or harm to that person or any other person.

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

Violation of privacy

10. (1) A person who, knowingly or without lawful excuse or justification, captures, publishes or transmits the image of a private area of a person without his or her consent, under circumstances violating the privacy of that person, commits an offence and is liable on summary conviction to a fine not exceeding two hundred thousand dollars or to a term of imprisonment not exceeding three years or to both.

(2) For the purposes of this section–

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

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

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

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

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

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

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

Misuse of encryption

11.(1) A person shall not for the purpose of the commission of an offence or concealment of incriminating evidence, encrypt in any electronic system any incriminating communication or data contained relating to the offence or incriminating evidence.

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

Child pornography

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

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

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

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

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

(d) facilitate the abuse of a child online;

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

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

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

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

(4) A person who contravenes subsection (2) commits an offence and is liable on conviction on indictment to a fine not exceeding two hundred thousand dollars or to a term of imprisonment not exceeding five years or to both and in the event of second or subsequent conviction to a fine not exceeding three hundred thousand dollars or to a term of imprisonment not exceeding twenty years or to both.

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

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

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

Sensitive electronic system

13. (1) A person shall not knowingly or without lawful excuse or justification disable or obtain access to a sensitive electronic system whether or not in the course of the commission of another offence under this Act.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction on indictment to a fine not exceeding three hundred thousand dollars or to a term of imprisonment not exceeding twenty years or to both.

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

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

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

(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, courts, public transportation or public key infrastructure;

(d) the protection of public safety including systems related to

essential emergency services such as police, civil defence and medical services ; or

(e) the purpose declared as such by the Minister by Order published in the *Gazette*.

Electronic terrorism

14. A person who–

(a) threatens the unity, integrity, security or sovereignty of Grenada or to strike terror in the people or any section of the people by–

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

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

(iii) introducing or causing to introduce any contaminant,

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

(b) knowingly or without lawful excuse or justification, gains access to an electronic system without lawful authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or electronic database that is restricted for reasons for the security of Grenada or foreign relations, or any restricted information, data or electronic database, with reasons to believe that such information, data or electronic database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of Grenada, the security of Grenada, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise,

commits an offence of electronic terrorism and is liable on conviction on indictment pursuant to the penalties prescribed in the Terrorism Act No. 16 of 2012.

Prank calls to law enforcement

15.(1) A person shall not make calls to any law enforcement authority or emergency services with the purpose of giving false and misleading information.

(2) A person making a call to any law enforcement or emergency services shall not–

(a) use a caller identification service to transmit misleading or inaccurate caller identification information service;

(b) mask their voice; or

(c) provide a fake phone number to the call recipient.

(3) A person who contravenes subsection (1) or (2) commits and offence and is liable on summary conviction to a fine not exceeding five thousand dollars or to a term of imprisonment not exceeding six months or to both.

Electronic stalking

16. (1) A person shall not knowingly or without lawful excuse or justification intimidate, coerce, insult or annoy another person using an electronic system.

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

Spoof and Spam

17. (1) A person shall not knowingly or without lawful excuse or justification establish a website or send an electronic message with a counterfeit source–

(a) so that the recipient or visitor of an electronic system will believe it to be an authentic source; or

(b) to attract or solicit a person or electronic system;

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

(2) A person shall not knowingly or without lawful excuse or justification-

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

(b) use a protected computer system to relay or retransmit multiple

electronic mail messages, with the intent to deceive or mislead users, or any electronic mail or internet service provider, as to the origin of such messages; or

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

(3) A person who contravenes subsection (1) or (2) commits an offence and is liable on summary conviction to a fine not exceeding two hundred thousand dollars or to a term of imprisonment not exceeding three years or to both.

Unauthorized access to code

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

(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding two hundred thousand dollars or to a term of imprisonment not exceeding three years or to both.

PART III
INVESTIGATIONS AND PROCEDURES

Preservation order

19. (1) Upon evidence sworn to by a police officer of the rank of Inspector, or above an application may be made to a Judge in Chambers for an order for the expeditious preservation of data that has been stored or processed by means of an electronic system, where there are reasonable grounds to believe that the data is vulnerable to loss or modification and where such data is required for the purposes of a criminal investigation or the prosecution of an offence.

(2) For the purposes of subsection (1), data includes traffic data and subscriber information.

(3) An order made under subsection (1) remains in force–

(a) for a period of thirty days;

(b) where prosecution is instituted, until the final determination of the case; or

(c) until such time as the Judge in Chambers determines necessary.

(4) The period specified for an order granted pursuant to sub-section (1) may be extended, upon an application by the applicant for a further of thirty days or period as may be specified in the order.

Disclosure of preserved data order

20. For the purposes of a criminal investigation or the prosecution of an offence, upon evidence sworn to by a police officer of the rank of Inspector, or above an application may be made to a Judge in Chambers for an order for the disclosure of–

(a) any preserved data, irrespective of whether one or more service providers were involved in the transmission of the data;

(b) sufficient data to identify the service providers and the path through which the data was transmitted; or

(c) the electronic key enabling access to or the interpretation of data.

Production order

21. (1) If the disclosure of data is required for the purpose of a criminal investigation or the prosecution of an offence, a police officer not below the rank of Inspector shall make a request of–

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

(b) a service provider offering its services to submit subscriber information in relation to the services in that service provider's possession and control.

(2) Where any material to which an investigation relates consists of data stored in an electronic system, disc, cassette, or on microfilm or preserved by any mechanical or electronic device, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible, audible or legible.

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

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

22. (1) Upon evidence sown by a police officer not below the rank of Inspector, that stored data would be relevant for the purposes of an investigation or the prosecution of an offence, the police officer may apply to a Judge in Chambers for the issue of a warrant to enter any premises to access, search and seize

that data.

(2) In the execution of a warrant under subsection (1), the powers of the police officer shall include the power to–

(a) access, inspect and check the operation of an electronic system;

(b) use or cause to be used an electronic system to search any data contained in or available to the electronic system;

(c) access any information, code or technology which has the capability of transforming or unscrambling encrypted data contained or available to an electronic system into readable and comprehensible format or text for the purpose of investigating any offence under this Act or any other offence which is disclosed in the course of the lawful exercise of the powers under this section;

(d) require a person in possession of the decryption information to grant the police officer access to such decryption information necessary to decrypt data required for required for the purpose of investigating the offence;

(e) seize or secure an electronic system.

(3) A person shall not knowingly or without lawful excuse or justification –

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

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

(4) A person who contravenes subsection (1) commits a summary offence and is liable on summary conviction to a fine not exceeding ten thousand dollars or to a term of imprisonment not exceeding one year or to both.

(5) For the purposes of this section–

"decryption information" means information or technology that enables a person to readily re-transform or unscramble encrypted data from its unreadable and incomprehensible format to its plain text version;

"encrypted data" means data which has been transformed or scrambled from its plain text version to an unreadable and incomprehensible format, regardless of the technique utilized for transformation or scrambling, and irrespective of

the medium in which such data occurs or can be found for the purposes of protecting the content of such data; and

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

Real time collection of traffic data

23. Where a police officer not below the rank of inspector has reasonable grounds to believe that any data would be relevant for the purposes of investigation and prosecution of an offence under this Act, the police officer may apply to a Judge in Chambers for an order–

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

(b) compelling a service provider, within its technical capabilities to effect such collection and recording referred to in paragraph (a) or assist the police officer to effect such collection and recording.

Mobile phone tracking in emergencies

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

(2) Pursuant to subsection (1), cases of emergency include cases of accidents, missing persons and the pursuit of suspects involved in murder, rape, kidnapping or any indictable offence punishable by at least five years imprisonment or more.

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

Arrest without warrant

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

Deletion

26. A Judge in Chambers may, on application by a police officer not below the rank of Inspector and being satisfied that an electronic system contains data that contains indecent photographs of children, order that the data be–

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

system; or

(b) expunged or the hardware upon which the data is stored be physically destroyed.

Limited use of data and information

27. A person shall not without lawful excuse or justification use or disclose data obtained pursuant to this Part for any purpose other than that for which the data was originally sought except–

(a) in accordance with any other enactment;

(b) in compliance with an order of the Judge in Chambers ;

(c) where the data is required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, assessing or collecting tax, duty or other monies owed or payable the Government;

(d) for the prevention of injury or other damage to the health of a person or serious loss or damage to property; or

(e) in the public interest.

No liability for service provider

28. A service provider shall not be liable for any actions taken or any information provided or disclosed to the Police or other law enforcement agencies in accordance with this Part.

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

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

(b) any action taken or data collected or recorded under the Order,

commits an offence and is liable on summary conviction to a fine not exceeding two hundred thousand dollars.

PART IV
MISCELLANEOUS

Institution of criminal proceedings

29. Criminal proceedings shall not be instituted under this Act except on information filed by, or with the consent of, the Director of Public Prosecutions.

Extraditable offences
30. An offence pursuant to Part II shall be considered to be extraditable crimes for which extradition may be granted or obtained under the Extradition Act Cap. 98.

Order for compensation
31. (1) A Court before which a person is convicted of an offence under this Act may make an order against that person for the payment by that person of sum of money fixed by the Court by way of compensation to a person for damage caused to his or her electronic system, program or data by the offence in respect of which the sentence is passed.

(2) A claim by a person for damages sustained by reason of the offence shall be deemed to have been satisfied to the extent of any amount which has been paid to him or her under an order for compensation, except that the order shall not prejudice any right to a civil remedy for the recovery of damages beyond the amount of compensation paid under the order.

(3) An order for compensation under this section shall be recoverable as a civil debt.

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

(2) In addition to making an order that obscene matter forming part of the subject matter of the offence is forfeited, the Court shall, where appropriate, order that the obscene matter be deleted from or no longer stored or made available through the electronic system.

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

Passed in the House of Representatives this day of , 2013.

.....
Clerk to the House of Representatives

Passed in the Senate this day of , 2013.

.....
Clerk to the Senate