No. 35 of 2016.

***Cybercrime Code Act* 2016.**

Certified on: 13 DEC 2016

No. 35 of 2016.

Cybercrime Code Act **2016.**

ARRANGEMENT OF SECTIONS.

PART I. - PRELIMINARY.

Division 1. - Compliance with Constitutional Requirements.

1. Constitutional requirements.
2. Interpretation -
"applications service"
"applications service provider"
"body corporate"
"child"
"communication"
"computer"
"computer program"
"content"
"content service"
"content service provider"
"court"
"criminally responsible"
"critical infrastructure"
"data"
"data traffic"
"device"
"electromagnetic"
"electronic communication"
"electronic output"
"electronic system"
"function"
"hacking"
"hinder"
"ict"
"ict service"
"ict service provider"
"image"
"interception"
"interference"
"malicious software"
"member of the Police Force"
"multiple electronic message"
"network"
"network service"
"network service provider"

"offence"
"online"
"person"
"pornography"
"possession"
"premises"
"principal magistrate"
"private place"
"property"
"public place"
"remote forensic tool"
"seize"
"sensitive data"
"spam"
"storage device"
"thing"
"this Act"
"utilise".

PART II. - JURISDICTION.

3. Application.
4. Effect of changes in law.
5. Age of criminal culpability.

PART III. - OFFENCES AND PENALTIES.

Division 1. - Offences Related to the Integrity of Data and Electronic Systems or Devices.

6. Unauthorised access or hacking.
7. Illegal interception.
8. Data interference.
9. System interference.
10. Data espionage.
11. Illegally remaining.

Division 2. - Computer Related Offences.

12. Electronic fraud.
13. Electronic forgery.
14. Electronic gambling or lottery by a child.
15. Identity theft.
16. Illegal devices.

Division 3. - Content Related Offences.

17. Pornography.
18. Child pornography.
19. Child online grooming.
20. Animal pornography.
21. Defamatory publication.
22. Cyber bullying.
23. Cyber harassment.

24. Cyber extortion.
25. Unlawful disclosure.
26. Spam.

Division 4. - Other Offences.

27. Cyber attack.
28. Online copyright infringement.
29. Online trade mark infringement.
30. Patent and industrial designs infringement.
31. Unlawful advertising.

PART IV. - PROCEDURE IN SEARCH, EVIDENCE, INVESTIGATION, ETC.

Division 1. - Authorised Search and Seizure.

32. Search.
33. Search powers.
34. Assistance.

Division 2. - Preservation of Evidence.

35. Production orders.
36. Expedited preservation.
37. Partial disclosure.
38. Restraining orders.

Division 3. - Powers of Investigation.

39. Authorised interception.
40. Collection of traffic data.
41. Forensic tools.

Division 4. - Evidence and Admissibility.

42. Judicial notice.
43. Electronic evidence.

PART V. - ICT SERVICE PROVIDERS.

44. Criminal liability of ICT service providers.
45. Disclosure of details of an investigation.

PART VI. - INTERNATIONAL CO-OPERATION.

46. Mutual assistance.
47. Extradition.

PART VII. - CERTAIN INDICTABLE OFFENCES, REGULATIONS, ETC.

48. Indictable offences triable summarily.
49. Rules, etc.
50. Regulations.

Schedules.

SCHEDULE 1.

SCHEDULE 2.

No. of 2016.

AN ACT

entitled

***Cybercrime Code Act* 2016,**

Being an Act to define and establish acts or omissions constituting offences committed through the use of information and communication technology or cybercrime, and for related purposes,

MADE by the National Parliament to come into operation in accordance with a notice in the National Gazette by the Head of State, acting on advice.

PART I. - PRELIMINARY.

Division 1. - Compliance with Constitutional Requirements.

1. CONSTITUTIONAL REQUIREMENTS.

(1) For the purposes of Section 41 of the ***Organic Law on Provincial Governments and Local-level Governments***, it is declared that this law relates to a matter of national interest.

(2) This Act, to the extent that it regulates or restricts a right or freedom referred to in Subdivision III.3.C. (*qualified rights*) of the ***Constitution***, namely -

(*a*) the right to freedom from arbitrary search and entry conferred by Section 44; and
(*b*) the right to freedom of expression conferred by Section 46; and
(*c*) the right to privacy conferred by Section 49; and
(*d*) the right to freedom of information conferred by Section 51; and
(*e*) the right to freedom of movement conferred by Section 52; and
(*f*) the right to protection from unjust deprivation of property conferred by Section 53,

of the ***Constitution***, that is necessary for the purpose of giving effect to the public interest in public safety, public order and public welfare and is reasonably justifiable in a democratic society having proper respect and regard for the rights and dignity of mankind taking into account the National Goals and Directive Principles and Basic Social Obligations, because of the risks cybercrime poses to public safety, public order and public welfare, as well as to the successful social and economic development of Papua New Guinea and its citizens.

2. INTERPRETATION.

In this Act, unless the contrary intention appears -

"applications service" means a service (for facilitating communications by means of guided or unguided electromagnetic energy) provided via one or more network services, but does not include such a service provided solely on the retail customer side of the network boundary;
"applications service provider" means an ICT Service Provider providing applications services;
"body corporate" means a company whether incorporated or unincorporated and includes government or public bodies, as well as terrorist groups or organisations;
"child" means, for the purposes of this Act, a person under the age of 18 years;
"communication" includes any communication of content -

(*a*) whether between persons, things, or persons and things; and
(*b*) in any combination or form including speech, music or other sounds, data, text, writing, signs, signals or images (animated or otherwise);

"computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, storage and display functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, or a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility;

"computer program" means data representing a set of instructions or statements that, when executed in a computer or other electronic device, causes the computer or electronic device to perform a function;

"content" means information in any combination or form including speech, music or other sounds, data, text, writing, signs, signals or images (animated or otherwise);

"content service" means -

(*a*) a broadcasting service; or

(*b*) an applications service which also supplies content;

"content service provider" means an ICT Service Provider providing content services;

"court" means the District Court or the National Court as appropriate;

"criminally responsible" has the same meaning as defined in Section 1 of the ***Criminal Code Act*** (Chapter 262);

"critical infrastructure" refers to the basic facilities, services, and installations needed for the functioning of a community, society or government including but not limited to transportation, communication systems, water supply, electricity supply, banking services, public institutions, including health facilities, post offices and education facilities;

"data" means any representation of facts, concepts, information (being either text, audio, video, audiovisual or images) machine readable code or instructions, in a form suitable for processing in an electronic system or device, including a program suitable to cause an electronic system or device to perform a function;

"data traffic" means any electronic data relating to a communication by means of an electronic system or device, generated by an electronic system or device 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;

"device" includes but is not limited to -

(*a*) components of an electronic system such as a computer, graphic card, mobile phone, or memory chip; or

(*b*) storage components such as a hard drive, memory card, compact disk, or tape; or

(*c*) input tools such as a keyboard, mouse, track pad, scanner, or digital camera; or

(*d*) output tools such as a printer, monitor, or screen;

"electromagnetic" means the interaction between electronic and magnetic fields producing energy that is propagated through free space or through a material medium in the form of electromagnetic waves such as radio waves, visible light, gamma rays, and also refers to the emission and transmission of such radiant energy;

"electronic communication" means a transmission of data in any form by means of guided or unguided electromagnetic energy;

"electronic output" means a statement or a representation whether in written, printed, pictorial, film, graphical, audio, visual, audiovisual or other form -

(*a*) produced by a computer or other electronic device; or

(*b*) displayed on the screen of a computer or other electronic device; or

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

"electronic system" means a system consisting of hardware or software, or a group of interconnected or related systems or devices, one or more of which, under a program, performs automatic (that is without direct human intervention) processing, generating, sending, receiving, or storing of data and includes, but is not limited to, electronic devices, the internet, input, output and storage facilities;

"function" means a task that includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer or other electronic device;

"hacking" means the act of exploring programs or determining the limitations of a computer, electronic system or device or network, for the purposes of gaining unauthorised access to such computer, electronic system or device, or network;

"hinder" means any act which interferes with the proper functioning of an electronic system or device, including but not limited to cutting or disrupting the electricity supply to that electronic system or device;

"ict" means information and communications technology;

"ict service" has the same meaning as 'ICT service' under Section 4 of the ***National Information and Communications Technology Act*** **2009** and includes, but is not limited to, the services provided by an ICT Service Provider;

"ict service provider" means a person who provides content, applications or network services or a combination of such services, including, but not limited to, those identified in Schedule 1 and includes their employees, servants, agents or assignees;

"image" means any picture, photograph, depiction, animation or visual representation of an object, scene, person, animal or abstraction;

"interception" means tapping into an electronic communication not directed to the one who is tapping into such communication for the purpose of acquiring, viewing or capturing such communication whether by earth bound (wired, cable) wireless, electronic optical, magnetic or other means during transmission through the use of any technical device;

"interference" means tampering with the integrity of information content or electronic data, or systems and includes one or more of the following:

(*a*) damaging; or
(*b*) deletion; or
(*c*) deterioration; or
(*d*) alteration; or
(*e*) suppression; or
(*f*) modification which includes additions, omissions and substitutions; or
(*g*) hindering,

of electronic data or electronic systems;

"malicious software" means malware or software that is intended to damage or disable an electronic system or device;

"member of the Police Force" means any member of the Royal Papua New Guinea Constabulary;

"multiple electronic message" means a mail message including e-mail and instant messaging sent to 50 or more recipients;

"network" means the interconnection, whether earth bound (wired, cable), wireless, or both of two or more electronic systems or other data processing devices, or a group of such interconnected or related devices;

"network service" means a service for carrying of communications, by means of guided or unguided electromagnetic energy, supplied between distinct geographic points at least one of which is located in Papua New Guinea, but does not include services provided solely on the retail customer side of the network boundary;

"network service provider" means an ICT Service Provider that provides a network service;

"offence" has the same meaning as Section 3 of the ***Criminal Code Act*** (Chapter 262);

"online" means accessing the internet and remaining there;
"person" means a natural person or body corporate;
"pornography" means -

(*a*) any photographic, film, video or other visual representation -
  (i) that shows a person who is, or who is depicted as, engaged in sexual activity; or
  (ii) which characteristics is the depiction of any part of the body of a person for or connoting a sexual purpose; or
(*b*) any audio representation of a person who is, or is represented as being, engaged in a sexual activity; or
(*c*) any written material, visual, audio or audiovisual representation that advocates, counsels or encourages sexual activity, irrespective of how or through what medium the representation has been produced, transmitted or conveyed and, without prejudice to the generality of the foregoing, includes any representation produced by or from computer graphics or other electronic or mechanical means; or
(*d*) a representation of sexual activity or sexual engagement with animals;

"possession" has the same meaning as "have in possession" under Section 1 of the ***Criminal Code Act*** (Chapter 262) and includes having under control in or on any website, whether for the use or benefit of the person in control whether or not another person has actual possession or custody of the thing or matter in question or whether or not the thing or matter in question is visible;
"premises" includes land, buildings, movable structures and any conveyance by land, water or air, or web hosting servers or websites;
"principal magistrate" means a magistrate duly empowered to preside in respect of committal proceedings or a Grade V Magistrate;
"private place" means a place other than a public place, including but not limited to a house, building, vessel, craft or vehicle;
"property" has the same meaning as in Section 1 of the ***Criminal Code Act*** (Chapter 262) and includes money;
"public place" means a place to which members of the public have access as a right, whether or not on payment of a fee and whether or not access to the place may be restricted at particular times or for particular purposes;
"remote forensic tool" means an investigative tool such as a software or a hardware installed on or applied with regard to an electronic system or device and used to perform tasks that include but are not limited to, keystroke logging or transmission of an Internet Protocol address;
"seize" includes -

(*a*) activating any onsite electronic system, device or electronic data storage media; or
(*b*) making and retaining a copy of electronic data, including by using onsite equipment; or
(*c*) maintaining the integrity of the relevant stored electronic data; or
(*d*) rendering inaccessible or removing electronic data in the accessed electronic system or device; or
(*e*) taking a printout of output of electronic data; or
(*f*) seizing or similarly securing an electronic system, device or part of it, or an electronic data storage medium;

"sensitive data" means any data or content whether in writing, images, audio, visual, audiovisual or in any other form -

(*a*) that is potentially detrimental or damaging to the person who is the subject of such information or personal data; or
(*b*) data that is classified or intended for restricted use or specified persons only; or

(*c*) data relating to the State, politics and the military, or corporate secrets, or data that is otherwise not available to the public;

"spam" means the transmission of harmful, fraudulent, misleading, illegal or otherwise unsolicited, electronic messages to a recipient without the express permission or approval of the recipient, or causing an electronic system or device to show such message or the involvement in falsified online user account registration or falsified domain name registration, for a commercial purpose;

"storage device" means any article or device from which information is capable of being reproduced, with or without the aid of any other article or device;

"thing" includes -

(*a*) an electronic system or device or part of an electronic system or device; or

(*b*) another electronic system or device, if -

(i) electronic data from that electronic system or device is available to the first electronic system or device being searched; and

(ii) there are reasonable grounds for believing that the electronic data sought is stored in the other electronic system or device; or

(*c*) an electronic data storage device; or

(*d*) an electronic equipment; or

(*e*) a network of devices;

"this Act" includes any schedules, regulations, rules or other subsidiary legislation made under this Act;

"utilise" includes -

(*a*) the development; or

(*b*) the adoption; or

(*c*) the purchase,

of a remote forensic tool.

PART II. - JURISDICTION

3. APPLICATION.

(1) Unless stated to the contrary, the provisions of the ***Criminal Code Act*** (Chapter 262) relating to -

(*a*) criminal practice and procedure; and

(*b*) jurisdiction, including Sections 12, 13 and 14; and

(*c*) punishments, including Sections 18 and 19,

apply to this Act.

(2) The provisions of this Act are in addition to and not in derogation of the ***Criminal Code Act*** (Chapter 262) or any other law relating to criminal matters, and where there are any inconsistencies between the provisions of this Act and the ***Criminal Code Act*** (Chapter 262) or any other law relating to criminal matters, the provisions of this Act shall apply.

4. EFFECT OF CHANGES IN LAW.

(1) A person cannot be punished for doing or omitting to do an act unless the act or omission constituted an offence under this Act in force when the offence occurred.

(2) This Act does not have retrospective effect on past commissions or omissions of acts that constituted an offence under this Act.

5. AGE OF CRIMINAL CULPABILITY.

(1) A child under the age of 10 years at the time of the act or omission that constitutes an offence under this Act is not criminally responsible for such act or omission.

(2) A child between the ages of 10 and 14 years is not criminally responsible for an act or omission, unless it is proved that at the time of doing the act or making the omission he had capacity to know that he ought not to do the act or make the omission.

(3) Where any of the offences in this Act are committed by a child between the ages of 10 and 18 years, the provisions of the ***Juvenile Justice Act* 2014** shall apply.

PART III. - OFFENCES AND PENALTIES.

Division 1. - Offences Related to the Integrity of Data and Electronic System or Devices.

6. UNAUTHORISED ACCESS OR HACKING.

(1) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, accesses or gains entry without authorisation, to the whole or any part of a protected or non-public electronic system or device, or data, is guilty of a misdemeanour.

Penalty: Imprisonment for a term not exceeding five years or a fine not exceeding K7,000.00, or both.

(2) Where the offence in Subsection (1) results in damage or loss to the whole or any part of an electronic system or device, or data, the offender is guilty of a crime.

Penalty: Imprisonment for a term not exceeding 15 years or a fine not exceeding K25,000.00, or both.

7. ILLEGAL INTERCEPTION.

(1) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, intercepts by technical or other means -

(*a*) any non-public transmission to, from or within an electronic system or device; or

(*b*) electromagnetic emissions from an electronic system or device,

not intended for him, is guilty of a crime.

Penalty: (*a*) A fine not exceeding K50,000.00 or imprisonment for a term not exceeding 15 years, or both; and

(*b*) In the case of a body corporate, a fine not exceeding K500,000.00.

(2) Where the offence under Subsection (1) is committed against State or Military transmissions, or transmissions of other sensitive data, the offender is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 25 years, or both; and

(*b*) In the case of a body corporate, a fine not exceeding K1,000,000.00.

8. DATA INTERFERENCE.

A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification or recklessly -

(*a*) damages or deteriorates data; or
(*b*) deletes data; or
(*c*) alters data; or
(*d*) renders data meaningless, useless or ineffective; or
(*e*) obstructs, interrupts or interferes with the lawful processing of data; or
(*f*) obstructs, interrupts or interferes with any person in their lawful use of data; or
(*g*) denies access to data to any person authorised to access it,

is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K20,000.00 or imprisonment for a term not exceeding 10 years, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K100,000.00.

9. SYSTEM INTERFERENCE.

(1) A person, who intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, or recklessly -

(*a*) hinders or interferes with the functioning of an electronic system or device; or
(*b*) hinders or interferes with a person's lawful use or operation of an electronic system or device,

is guilty of a misdemeanour.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K10,000.00 or imprisonment for a term not exceeding 10 years, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K100,000.00.

(2) Where the offence is committed against an electronic system or device that is exclusively for the use or operation of critical infrastructure, or in the case where such electronic system or device is not exclusively for the use or operation of critical infrastructure, but is otherwise used in connection with the operation of critical infrastructure, and such conduct -

(*a*) affects the use of critical infrastructure; or
(*b*) impacts the operation of critical infrastructure,

the offender is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 25 years, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K1,000,000.00 and K25,000.00 for each subsequent day the critical infrastructure remains inoperable.

10. DATA ESPIONAGE.

(1) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, whether for his own use or for the use of another person, accesses or obtains protected data which is not meant for him, and which is protected against unauthorised access, is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 30 years, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K500,000.00.

(2) Where the offence under Subsection (1) is committed against State secrets or Military secrets, or sensitive data, the offender is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 30 years, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K1,000,000.00.

11. ILLEGALLY REMAINING.

A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification or recklessly, remains logged into or continues to use an electronic system or device, or part of an electronic system or device, without authorisation or after his authorised use of the electronic system or device has expired, is guilty of a misdemeanour.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K10,000.00 or imprisonment for a term not exceeding seven years, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K50,000.00.

Division 2. - Computer Related Offences.

12. ELECTRONIC FRAUD.

(1) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification -

(*a*) inputs, alters, deletes, or suppresses electronic data; or
(*b*) otherwise interferes with the functioning of an electronic system or device,

for the purpose of deceiving or depriving another person of their property for his own gain or that of another person, is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 25 years, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K1,000,000.00.

(2) A person who, without lawful excuse or justification, or in excess of a lawful excuse or justification, conspires with another person to commit, or attempts to commit an offence under this section, is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K25,000.00 or imprisonment for a term not exceeding 15 years, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K500,000.00.

13. ELECTRONIC FORGERY.

(1) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification -

(*a*) inputs, alters, deletes, or suppresses electronic data; or
(*b*) otherwise interferes with the functioning of an electronic system or device,

for the purpose of creating or generating inauthentic data that it may be considered or acted upon for lawful purposes as if it were authentic, regardless of whether the data is directly readable or intelligible, is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 25 years, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K1,000,000.00.

(2) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, conspires with another person to commit, or attempts to commit an offence under this section, is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K15,000.00 or imprisonment for a term not exceeding 15 years, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K500,000.00.

14. ELECTRONIC GAMBLING OR LOTTERY BY A CHILD.

(1) A child who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, uses an electronic system or device to participate in a lottery or any gaming activity, whether or not, by means of the internet, is guilty of a misdemeanour.

Penalty: (*a*) Subject to the ***Juvenile Justice Act* 2014**, imprisonment for a term not exceeding seven years; or
(*b*) Prohibition from accessing and using ICTs or electronic system or devices for the term of imprisonment imposed plus an additional two years; or
(*c*) Both Paragraphs (*a*) and (*b*).

(2) A gaming operator, who knowingly or recklessly, and without lawful excuse or justification, or in excess of a lawful excuse or justification, makes available to a child, lottery or other gaming activity through an electronic system or device, is guilty of a crime.

Penalty: (*a*) In the case of natural person, a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 25 years, or both; and
(*b*) In the case of a body corporate, fine not exceeding K1,000,000.00.

(3) For the purposes of this section -

"gaming or gaming activity" means all forms of gaming regulated under the ***Gaming Control Act* 2007**;

"gaming operator" means the operator of an approved game under the ***Gaming Control Act* 2007**;

"lottery" means a scheme for distributing prizes by lot or chance.

15. IDENTITY THEFT.

A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, uses an electronic system or device -

(*a*) to access; or
(*b*) to manipulate; or
(*c*) to possess; or
(*d*) to use; or
(*e*) to transfer,

a means of identification of another person without the authorisation of that other person, is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K15,000.00 or imprisonment for a term not exceeding 10 years, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K100,000.00.

16. ILLEGAL DEVICES.

(1) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, designs, produces, sells, procures for use, imports, exports, distributes or otherwise makes available -

(*a*) an electronic system or device, or thing that is designed or adapted; or

(*b*) a password, access code or similar data by which the whole or any part of an electronic system or device, or thing is capable of being accessed,

for the purpose of committing an offence defined by other provisions of Part III of this Act, is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K25,000.00 or imprisonment for a term not exceeding 15 years or, both; and

(*b*) In the case of a body corporate, a fine not exceeding K100,000.00.

(2) It is a defence to a charge under this section where the design, production, sale, procurement for use, import, distribution or otherwise making available, or possession of devices referred to in Subsection (1), is for authorised testing or protection of an electronic system or device, or for law enforcement purposes.

(3) Whether an illegal device referred to in Subsection (1) is for authorised testing, protection of an electronic system or device, or law enforcement purposes, is a question of fact.

Division 3. - Content Related Offences.

17. PORNOGRAPHY.

(1) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, uses an electronic system or device to -

(*a*) produce pornography for the purpose of its distribution; or

(*b*) offer or make available pornography for public viewing; or

(*c*) distribute or transmit pornography to another person or the public; or

(*d*) procure or obtain access to pornography whether or not by downloading it or transmitting it either to himself or another person for the purpose of giving effect to or facilitating the commission of any of the offences in Paragraphs (*b*) or (*c*) above,

is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K25,000.00 or imprisonment for a term not exceeding 15 years, or both; and

(*b*) In the case of a body corporate, a fine not exceeding K100,000.00.

(2) It is a defence to a charge for an offence under Subsection (1)(*b*), (*c*) and (*d*) if the pornography was for a ***bona fide*** law enforcement purpose or for the benefit of the public.

(3) Whether the doing of an act referred to in Subsection (1) is for the benefit of the public, is a question of fact.

18. CHILD PORNOGRAPHY.

(1) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, uses an electronic system or device to commit any of the offences prescribed under Sections 229R, 229S and 229T of the ***Criminal Code Act*** (Chapter 262), is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 25 years, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K1,000,000.00.

(2) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, uses an electronic system or device to access child pornography, whether or not for the purpose of downloading or transmitting it either to himself or another person, or, for the purpose of giving effect to or facilitating the commission of any of the offences in Subsection (1), is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 25 years, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K1,000,000.00.

(3) It is a defence to a charge for an offence under this section if the child pornography was for a ***bona fide*** law enforcement purpose or for the benefit of the public.

(4) Whether the doing of an act referred to in this section is for the benefit of the public, is a question of fact.

(5) For the purposes of this section, if child pornography is stored for a ***bona fide*** law enforcement purpose, all traces, copies, or storage of such pornographic material shall be removed, deleted or otherwise destroyed once it is no longer lawfully required.

19. CHILD ONLINE GROOMING.

(1) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, uses an electronic system or device to befriend, invite, induce, persuade, or in any way procure, or offer to engage a child in -

(*a*) sexual intercourse or sexual contact; or
(*b*) a sexual or obscene performance; or
(*c*) any other sexual conduct,

is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 25 years, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K500,000.00.

(2) Where the offence under Subsection (1) is committed in respect of a child under the age of 16 years, the offender is guilty of a crime.

Penalty: (*a*) In the case of a natural person, subject to Section 19 of the ***Criminal Code Act*** (Chapter 262), imprisonment for life; and
(*b*) In the case of a body corporate, a fine not exceeding K1,000,000.00.

(3) A person who knowingly receives any financial or other reward, favour, benefit, compensation, or any other gain from the commission of an offence under this section, is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 25 years, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K1,000,000.00.

20. ANIMAL PORNOGRAPHY.

A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, or recklessly, uses an electronic system or device to -

(*a*) produce; or
(*b*) offer or make available; or
(*c*) distribute or transmit; or
(*d*) procure or obtain for himself or for another person, access to, pornography of himself or of another person engaged in sexual activity with an animal or animals; or
(*e*) obtain access to animal pornography whether or not by downloading or transmitting it either to himself or another person, for the purpose of giving effect to, or facilitating the commission of any one or more of the offences in Paragraphs (*b*), (*c*) and (*d*) above,

is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K25,000.00 or imprisonment for a term not exceeding 15 years, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K100,000.00.

21. DEFAMATORY PUBLICATION.

(1) For the purposes of this Section -

"publication" means using an electronic system or device to make publicly available defamatory material to persons other than the defamed person and includes electronic writings, images, audio, visual or audiovisual recordings;

"defamatory material" means an imputation, whether directly expressed or by implication, insinuation, innuendo or irony, that concerns a person or a member of his family, whether living or dead, with the intention of -

(i) injuring the reputation of that person; or
(ii) injuring the profession or trade of that person; or
(iii) inducing other people to shun, avoid, ridicule or despise that person.

(2) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, or recklessly, uses an electronic system or device to publish defamatory material concerning another person, is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K25,000.00 or a term of imprisonment not exceeding 15 years, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K100,000.00.

(3) Where the offence under Subsection (2) is committed with the knowledge that the published defamatory material is false, the offender is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K50,000.00 or imprisonment for a term not exceeding 25 years, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K500,000.00.

(4) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, or recklessly, uses an electronic system or device to publish, or directly or indirectly threaten to publish or offer to prevent the publication of, defamatory material concerning another, for the purpose of -

(*a*) extorting from that other person or any other person; or
(*b*) inducing a person to -

(i) give or confer; or
(ii) procure or to attempt to procure,
upon or for a person, any property or benefit of any kind, is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 25 years, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K1,000,000.00.

(5) It is a defence to a charge for an offence under this section that the defamatory material published -

(*a*) was true; or
(*b*) was for the benefit of the public; or
(*c*) constituted a fair comment; or
(*d*) was made in good faith.

(6) Whether or not the publication complained of is true, or was made for the benefit of the public, or constitutes fair comment, or was made in good faith, is a question of fact.

(7) Where the defence of good faith is raised under Subsection (5)(*d*), the burden of proof shifts to the party alleging the absence of good faith.

(8) Where the defamatory publication consists of or relates to electronic writings, images, audio, visual or audiovisual recordings of a sexual nature or depicting sexual conduct, the defence of truth is not available to the offender notwithstanding that the published defamatory material complained of was produced with the knowledge or consent of the person defamed.

(9) The provisions of Section 362E of the ***Criminal Code Act*** (Chapter 262), relating to protection of matters of public interest, apply to this section.

(10) For the purpose of Subsection (9), "public meeting" referred to in Section 362E of the ***Criminal Code Act*** (Chapter 262) includes online discussion forums whether or not they are featured on social networking sites.

22. CYBER BULLYING.

(1) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, or recklessly, uses an electronic system or device whether or not it is connected to the internet (with or without the aid of electronic writings, images, audio, visual or audiovisual recordings, or the exchange of messages) to -

(*a*) initiate; or
(*b*) facilitate; or
(*c*) participate in,
any communication or online discussion or posts with or regarding a child, directly or indirectly (with or without any exchange of messages or electronic writings, images, audio, visual or audiovisual recordings) with the child subject of the bullying for the purpose of -

(i) bullying, intimidating, threatening, demeaning, ridiculing or stalking, or causing emotional distress; or
(ii) supporting such repeated acts under Subparagraph (i),
in respect of that child, is guilty of a misdemeanour.

Penalty: (*a*) In the case of a child offender, subject to the ***Juvenile Act*** **2014** -
(i) detention for a term not exceeding three years; or
(ii) prohibition from accessing and using ICTs or electronic system or devices for the term of detention imposed plus an additional two years; or
(iii) both Subparagraphs (i) and (ii); and
(*b*) In the case of an adult offender -
(i) imprisonment for a term not exceeding seven years; or
(ii) prohibition from accessing and using ICTs or electronic system or devices for the term of imprisonment imposed plus an additional two years; or
(iii) both Subparagraphs (i) and (ii).

(2) Where the offence under Subsection (1) results in psychological or physical harm, the offender is guilty of a crime.

Penalty: (*a*) In the case of a child offender, subject to the ***Juvenile Justice Act*** **2014** -
(i) detention for a term not exceeding five years; or
(ii) prohibition from accessing and using ICTs or electronic system or devices for the term of detention imposed plus an additional two years; or
(iii) both Subparagraphs (i) and (ii); and
(*b*) In the case of an adult offender -
(i) imprisonment for a term not exceeding 25 years; or
(ii) prohibition from accessing and using ICTs or electronic system or devices for the term of imprisonment imposed plus an additional two years; or
(iii) both Subparagraphs (i) and (ii).

(3) Where the offence in Subsection (1) results in death, the offender is guilty of a crime.

Penalty: (*a*) In the case of a child offender, subject to the ***Juvenile Justice Act*** **2014** and Section 19 of the ***Criminal Code Act*** (Chapter 262) -
(i) imprisonment for life; and
(ii) prohibition from accessing and using ICTs or electronic systems or devices for the term of imprisonment imposed; and
(*b*) In the case of an adult offender, subject to Section 19 of the ***Criminal Code Act*** (Chapter 262) -
(i) imprisonment for life; and
(ii) prohibition from accessing and using ICTs or electronic systems or devices for the term of imprisonment imposed.

23. CYBER HARASSMENT.

(1) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, or recklessly, uses an electronic system or device whether or not it is connected to the internet (with or without the aid of electronic writings, images, audio, visual or audiovisual recordings, or the exchange of messages) to -
(*a*) initiate; or
(*b*) facilitate; or

(*c*) participate in,

any communication or online discussion or posts regarding another person, directly or indirectly (with or without any exchange of messages or electronic writings, images, audio, visual or audiovisual recordings) with the person harassed, for the purpose of -

(i) coercing, intimidating, threatening, harassing, stalking, or causing emotional distress; or

(ii) supporting such repeated acts under Subparagraph (i),

in respect of that person, is guilty of a misdemeanour.

Penalty: (*a*) In the case of a child offender, subject to the ***Juvenile Justice Act* 2014** -

(i) detention for a term not exceeding three years; or

(ii) prohibition from accessing and using ICTs or electronic system or devices for the term of detention imposed plus an additional two years; or

(iii) both Subparagraphs (i) and (ii); and

(*b*) In the case of an adult offender -

(i) imprisonment for a term not exceeding seven years; or

(ii) prohibition from accessing and using ICTs or electronic system or devices for the term of imprisonment imposed plus an additional two years; or

(iii) both Subparagraphs (i) and (ii).

(2) Where the offence under Subsection (1) results in psychological harm or physical injury, the offender is guilty of a crime.

Penalty: (*a*) In the case of a child offender, subject to the ***Juvenile Justice Act* 2014** -

(i) detention for a term not exceeding five years; or

(ii) prohibition from accessing and using ICTs or electronic system or devices for the term of imprisonment imposed plus an additional two years; or

(iii) both Subparagraphs (i) and (ii); and

(*b*) In the case of an adult offender -

(i) imprisonment for a term not exceeding 10 years; or

(ii) prohibition from accessing and using ICTs or electronic system or devices for the term of imprisonment imposed plus an additional two years; or

(iii) both Paragraphs (i) and (ii).

(3) Where the offence under Subsection (2) results in death, the offender is guilty of a crime.

Penalty: (*a*) In the case of a child offender, subject to the ***Juvenile Justice Act* 2014** and Section 19 of the ***Criminal Code Act*** (Chapter 262) -

(i) imprisonment for life; and

(ii) prohibition from accessing and using ICTs or electronic systems or devices for the term of detention imposed; and

(*b*) In the case of an adult offender, subject to Section 19 of the ***Criminal Code Act*** (Chapter 262) -

(i) imprisonment for life; and

(ii) prohibition from accessing and using ICTs or electronic devices for the term of imprisonment imposed.

(4) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, or recklessly, uses an electronic system or device whether or not it is connected to the internet (with or without the aid of electronic writings, images, audio, visual or audiovisual recordings) to -

(*a*) authorise, facilitate or enable; or
(*b*) write, post or effect; or
(*c*) entertain, encourage or participate in,

the posting of commentary, whether or not it is directed at anyone in particular, using or connoting profanity or obscenity, or language or imagery that is vulgar, or otherwise unacceptable or which grossly offends against accepted standards of public decency, to any person reading such post or commentary, is guilty of a crime.

Penalty: (*a*) In the case of a child offender, subject to the ***Juvenile Justice Act*** **2014** -
(i) detention for a term not exceeding three years; or
(ii) a fine not exceeding K5,000.00; or
(iii) prohibition from accessing and using ICTs or electronic systems or devices for the term of detention imposed plus an additional two years; or
(iv) all of Subparagraphs (i), (ii) and (iii); or

(*b*) In the case of an adult offender -
(i) imprisonment for a term not exceeding 10 years; or
(ii) a fine not exceeding K15,000.00; or
(iii) prohibition from accessing and using ICTs or electronic systems or devices for the term of imprisonment imposed plus an additional two years; or
(iv) all of Subparagraphs (i), (ii) and (iii); or

(*c*) In the case of a body corporate, a fine not exceeding K50,000.00.

24. CYBER EXTORTION.

(1) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, uses an electronic system or device to -

(*a*) upload or threaten to upload; or
(*b*) deploy or threaten to deploy; or
(*c*) input or threaten to input,

into an electronic system or device, software designed to restrict, disrupt or in any way hinder the operation of or access to an electronic system or device, for the purpose of procuring monetary or other benefit for himself or another person, is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K50,000.00 or imprisonment for a term not exceeding 25 years, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K500,000.00.

(2) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, uploads, deploys, inputs or threatens to upload, deploy or input, into an electronic system or device, electronic writings, images, audio, visual or audiovisual recordings, for the purpose of -

(*a*) accusing or threatening to accuse or cause the accusation of, another person of committing an indictable offence or any other offence under this Act, the ***Criminal Code Act*** (Chapter 262) or any other law; or
(*b*) otherwise exposing sensitive data or compromising of confidential information with intent to procure monetary or other gain for himself or another person,

is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 25 years, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K1,000,000.00.

(3) It is immaterial whether the person accused or threatened to be accused has committed the offence or act of which he is being accused or threatened to be accused.

25. UNLAWFUL DISCLOSURE.

(1) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, or recklessly, uses an electronic system or device to disclose any confidential or classified communication (whether content, data or electronic output) or sensitive data, is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K20,000.00 or imprisonment for a term not exceeding 15 years, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K100,000.00.

(2) Where the offence is committed by a person with lawful authority, custody, access or control, in respect of such confidential or classified communication or sensitive data, the offender is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 25 years, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K500,000.00.

(3) It is a defence to a charge for an offence under this section to prove that it was for the benefit of the public that confidential or classified communication or sensitive data was disclosed.

(4) Whether the unlawful disclosure under this section is for the benefit of the public, is a question of fact.

26. SPAM.

A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, or recklessly, uses an electronic system or device -

(*a*) to initiate the transmission of multiple electronic messages with the intent to deceive or mislead users; or
(*b*) which is password protected to relay or retransmit multiple electronic messages, with the intent to deceive or mislead users, or any ICT Service Provider, as to the origin of such messages; or
(*c*) to materially falsify header information in multiple electronic messages with the intent of initiating the transmission of such messages,

is guilty of an offence.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K5,000.00 or imprisonment for a term not exceeding 12 months, or both; and
(*b*) In the case of a body corporate, a fine not exceeding K100,000.00.

Division 4. - Other Offences.

27. CYBER ATTACK.

(1) A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, inputs or deploys malicious software into an electronic system or device, data, infrastructure, or program resident or transiting within an electronic system or device, for the purpose of

altering or causing harm to, or, disrupting, degrading, destroying an electronic system or device, data, infrastructure, or program, is guilty of a crime.

Penalty: (*a*) In the case of a natural person -
(i) imprisonment for a term not exceeding 15 years; or
(ii) a fine not exceeding K50,000.00; or
(iii) prohibition from accessing and using ICTs or electronic systems or devices for the term of imprisonment imposed plus an additional two years; or
(iv) all or any of Subparagraphs (i), (ii) or (iii); and
(*b*) In the case of a body corporate, a fine not exceeding K500,000.00.

(2) Where the offence under Subsection (1) is committed against a critical infrastructure, the offender is guilty of a crime.

Penalty: (*a*) In the case of a natural person -
(i) imprisonment for a term not exceeding 25 years; or
(ii) a fine not exceeding K100,000.00; or
(iii) prohibition from accessing and using ICTs or electronic systems or devices for the term of imprisonment imposed plus an additional two years; or
(iv) all or any of Subparagraphs (i), (ii) or (iii); and
(*b*) In the case of a body corporate, a fine not exceeding K1,000,000.00.

28. ONLINE COPYRIGHT INFRINGEMENT.

A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, or recklessly, uses an electronic system or device, and knowingly and repeatedly -
(*a*) infringes; or
(*b*) authorises the infringement of; or
(*c*) facilitates or enables the infringement of,
a right protected under the ***Copyright and Neighbouring Rights Act* 2000** or any other laws relating to copyright, is guilty of a crime.

Penalty: (*a*) In the case of a natural person -
(i) imprisonment for a term not exceeding 15 years; or
(ii) a fine not exceeding K100,000.00; or
(iii) prohibition from accessing and using ICTs or electronic system or devices for the term of imprisonment imposed plus an additional two years; or
(iv) all or any of Subparagraphs (i), (ii) or (iii); and
(*b*) In the case of a body corporate, a fine not exceeding K1,000,000.00.

29. ONLINE TRADEMARK INFRINGEMENT.

A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, or recklessly, uses an electronic system or device, and knowingly or repeatedly -
(*a*) sells; or
(*b*) exposes for sale,
goods or services to which a forgery of a registered trademark is falsely applied in contravention of the ***Trademarks Act*** (Chapter 385), or any other laws relating to trademarks, is guilty of a crime.

Penalty: (*a*) In the case of a natural person -
(i) imprisonment for a term not exceeding 15 years; or
(ii) a fine not exceeding K100,000.00; or
(iii) prohibition from accessing and using ICTs or electronic system or devices for the term of imprisonment imposed plus an additional two years; or
(iv) all or any of Subparagraphs (i), (ii) or (iii); and
(*b*) In the case of a body corporate, a fine not exceeding K1,000,000.00.

30. PATENT AND INDUSTRIAL DESIGNS INFRINGEMENT.

A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, or recklessly, uses an electronic system or device, and knowingly or repeatedly commits an act or omission which contravenes the ***Patents and Industrial Designs Act* 2000** or any other law relating to patents and industrial designs, is guilty of a crime.

Penalty: (*a*) In the case of a natural person -
(i) imprisonment for a term not exceeding 15 years; or
(ii) a fine not exceeding K100,000.00; or
(iii) prohibition from accessing and using ICTs or electronic system or devices for the term of imprisonment imposed plus an additional two years; or
(iv) all or any of Subparagraphs (i), (ii) or (iii); and
(*b*) In the case of a body corporate, a fine not exceeding K1,000,000.00.

31. UNLAWFUL ADVERTISING.

A person who, intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, or recklessly, uses an electronic system or device, to advertise or promote an act or omission that would constitute an offence under this Act or any other law, is guilty of a crime.

Penalty: (*a*) In the case of a natural person -
(i) imprisonment for a term not exceeding 10 years; or
(ii) a fine not exceeding K20,000.00; or
(iii) prohibition from accessing and using ICTs or electronic system or devices for the term of imprisonment imposed plus an additional two years; or
(iv) all or any of Subparagraphs (i), (ii) or (iii); and
(*b*) In the case of a body corporate, a fine not exceeding K500,000.00.

PART IV. - PROCEDURE IN SEARCH, EVIDENCE, INVESTIGATION, ETC.

Division 1. - Authorised Search and Seizure.

32. SEARCH.

(1) Where a member of the Police Force believes that there are reasonable grounds for suspecting that there is in a private place, a data or thing that may provide evidence of the commission of an offence, he may, under a warrant issued under Subsection (2), enter the private place and -
(*a*) search the private place; or
(*b*) seize any such data or thing.

(2) Where it appears to a Magistrate, by information on oath, that there are reasonable grounds for suspecting that there is, in a private place, a data or thing that may provide evidence of the commission of an offence, he may issue a warrant directing a member of the Police Force named in the warrant, or all members of the Police Force to search the private place and to seize any such data or thing and take it before a Magistrate to be dealt with according to law.

(3) A warrant under Subsection (2) must be executed by day unless, by the warrant, the Magistrate specifically authorises it to be executed by night.

(4) Any data or thing seized under Subsection (2) may be detained by a Magistrate, and when it is no longer required as evidence, it may be destroyed under an order of a Magistrate.

33. SEARCH POWERS.

In addition to the powers under the ***Search Act*** (Chapter 341), where a member of the Police Force suspects, on reasonable grounds, that a thing may provide evidence of the commission of an offence, he may, in executing a warrant, exercise the following powers:

(*a*) operate the electronic system or device, or direct an occupant of the private place to operate the electronic system or device in order to determine whether it contains data or a thing that could be seized; or

(*b*) operate the electronic system or device, or direct an occupant of the private place to operate the electronic system or device to access data (including data stored on a separate storage device or data not held at the private place) or thing if the member of the Police Force believes, on reasonable grounds, that the data or thing might be data or thing that could be seized; or

(*c*) copy the data or thing that could be seized to a storage device and take the storage device from the place; or

(*d*) copy the data or thing that could be seized in documentary form and seize the produced documents; or

(*e*) move any electronic system or device, or thing, at the place subject of the search, to another place for examination in order to determine whether it contains data that could be seized if -

(i) it is significantly more practicable to do so having regard to the task it will take to copy the data and the availability of the technical expertise that will be required to do so; and

(ii) there are reasonable grounds to suspect that the electronic system or device, or thing contains data that could be seized; or

(*f*) do anything reasonably necessary to prevent loss, destruction or damage to anything connected with the offence; or

(*g*) use other members of the Police Force or other persons authorised under the warrant as reasonably necessary for the search.

34. ASSISTANCE.

A member of the Police Force may, upon production of a search warrant obtained under Sections 32 and 33, require a person who is not a suspect of an offence but is in possession or control of an electronic system or device, data or thing that is reasonably required for the purposes of an investigation or proceeding, to enable and assist him, if required, to –

(*a*) access and use an electronic system or device, data or thing; or

(*b*) obtain and copy data; or

(*c*) use an electronic system or device, or thing to make copies; or

(*d*) obtain an output from an electronic system or device, or thing in a format that can be read.

Division 2. - Preservation of Evidence.

35. PRODUCTION ORDERS.

Where specified data or a printout is reasonably required for the purposes of an investigation or proceedings, the Court may, on application by a member of the Police Force or the Public Prosecutor, as the case may be, order -

(*a*) a person in control of an electronic system or device, or thing to produce specified data or a printout of such data; or

(*b*) an ICT Service Provider to produce information about persons who subscribe to or use its services.

36. EXPEDITED PRESERVATION.

(1) Where a member of the Police Force, has reasonable grounds to suspect that -

(*a*) data stored in an electronic system or device, or thing is required for the purpose of an investigation or proceeding; and

(*b*) there is a risk that the data, electronic system or device, or thing may be destroyed or rendered inaccessible,

he may, by written notice, require a person in control of the data, electronic system or device, or thing to ensure that the data specified in the notice be preserved for a period of up to 14 days.

(2) Subject to Subsection (3), the Magistrate may, upon application by the member of the Police Force, authorise an extension for a further 14 days from the expiry of the initial 14 days.

(3) An application under Subsection (2) shall be made at anytime within the initial 14 days.

(4) A person who fails to comply with a request under Subsection (1) is guilty of an offence.

Penalty: (*a*) In the case or a natural person, a fine not exceeding K10,000.00 or imprisonment for a term not exceeding 12 months, or both; and

(*b*) In the case of a body corporate, a fine not exceeding K100,000.00.

37. PARTIAL DISCLOSURE.

Where the Court is satisfied, on application by a member of the Police Force or the Public Prosecutor, as the case may be, that specified data stored in an electronic system or device, or thing is required for the purpose of an investigation or proceeding, the Court may order such person to disclose sufficient traffic data about a specified communication to identify -

(*a*) the ICT Service Providers involved; and

(*b*) the path through which the communication was transmitted.

38. RESTRAINING ORDERS.

Where the Court, on application by a member of the Police Force or the Public Prosecutor, as the case may be, is satisfied that there are sufficient grounds to believe that an electronic system or device, data or thing reasonably required for the purposes of an investigation or proceeding, is likely to be removed, destroyed, deleted or otherwise tampered with or dealt with, it may make an order restraining or preventing such removal, destruction, deletion or tampering or dealing with such electronic system or device, data or thing.

Division 3. - Powers of Investigation.

39. AUTHORISED INTERCEPTION.

Where, on application by a member of the Police Force or the Public Prosecutor, as the case may be, the Court is satisfied upon sworn evidence that there are sufficient grounds to suspect that data or communication is reasonably required for the purposes of an investigation or proceeding, the Court shall -

(*a*) order an ICT Service Provider whose service is available in the country to collect or record through application of technical or other means, to permit or assist a member of the Police Force with the collection or recording of data or communication associated with specified communications transmitted by means of an electronic system or device; or

(*b*) authorise a member of the Police Force to collect or record that data through application of technical or other means.

40. COLLECTION OF TRAFFIC DATA.

Where, on application by a member of the Police Force or the Public Prosecutor, as the case may be, the Court is satisfied upon sworn evidence that traffic data associated with a specified communication is reasonably required for the purposes of an investigation or proceeding, the Court may order a person in control of such data to -

(*a*) collect or record traffic data associated with a specified communication during a specified period; or

(*b*) enable and assist a member of the Police Force to collect or record that data.

41. FORENSIC TOOLS.

(1) In an investigation of an offence under this Act, if relevant evidence cannot be collected by applying other instruments under this Part, then the Court, on application by a member of the Police Force or the Public Prosecutor, as the case may be, on being satisfied upon sworn evidence that such evidence is reasonably required for the purposes of an investigation or proceeding, authorise a member of the Police Force to -

(*a*) install such software or hardware on the suspect's electronic system or device in order to collect the relevant evidence; and

(*b*) use a remote forensic software or hardware,

only for the specific task required for the investigation.

(2) The authorisation to install the software or hardware may include remotely accessing the suspect's electronic system or device.

(3) The application under Subsection (1) shall contain the following information:

(*a*) the name and address of the suspect; and

(*b*) description of the targeted electronic system or device; and

(*c*) description of the intended measure, extent and duration of the utilisation; and

(*d*) the grounds for the use of such software or hardware.

(4) An order made under Subsection (1) shall include a requirement that any modifications to the electronic system or device of the suspect are limited to those relevant to the investigation and that any changes if possible can be undone at the end of the investigation.

(5) During the investigation it is necessary to record -

(*a*) the technical means used and the time and date of the application; and

(*b*) the identification of the electronic system or device and details of its modifications; and

(*c*) any information obtained.

(6) Information obtained by the use of such software or hardware is to be protected against any unauthorised modification, deletion or access.

(7) The duration of an order made under Subsection (1) shall not exceed six months.

(8) Where an order under Subsection (1) is discharged, the software or hardware installed shall immediately be removed.

(9) The Court may revoke an order under Subsection (1) where it is satisfied, on reasonable grounds, that in discharging the order, a member of the Police Force acted in excess of its terms.

(10) Where the installation process requires physical access to a private place, the requirements of Sections 32 and 33 shall be complied with.

(11) In an application under Subsection (1), the Court may order an ICT Service Provider to assist with the installation process.

Division 4. - Evidence and Admissibility.

42. JUDICIAL NOTICE.

(1) The Court shall take judicial notice of electronic seals, electronic signatures or electronic certificates, or any other forms of electronic verification.

(2) Where relevant, Part II of the ***Evidence Act*** (Chapter 48) relating to Judicial Notice applies to this Act.

43. ELECTRONIC EVIDENCE.

(1) In the trial of an offence under this Act, the fact that evidence has been generated or stored electronically or has resulted from an electronic system or device does not of itself prevent that evidence from being admissible in Court.

(2) Evidence required for the purposes of this Act shall be governed by the provisions of the ***Evidence Act*** (Chapter 48).

PART V. - ICT SERVICE PROVIDERS.

44. CRIMINAL LIABILITY OF ICT SERVICE PROVIDERS.

(1) An ICT Service Provider which -

(*a*) intentionally or knowingly, and without lawful excuse or justification or in excess of a lawful excuse or justification, monitors the information which they transmit or store on behalf of their users or actively seek facts or circumstances indicating illegal activity by their users; or

(*b*) intentionally or without lawful excuse or justification, or in excess of a lawful excuse or justification, initiates or aides in facilitating the action which results in the commission of an offence under this Act or which results in the contravention of any other law in force in Papua New Guinea; or

(*c*) knowingly or upon knowledge of criminal investigations or proceedings, undertakes or omits to undertake an act, thereby concealing, preventing, or frustrating the criminal investigations or proceedings; or

(*d*) does not comply with an order by the Court requiring it to -

(i) assist law enforcement in the prevention, investigation, or prosecution of an offence under this Act or any other law in force in Papua New Guinea; or

(ii) terminate or prevent a certain action which would result in the commission or continuation of an offence already committed under this Act or any other law in force in Papua New Guinea; or

(*e*) negligently allows an employee to commit an offence under Paragraph (*a*), (*b*), (*c*) or (*d*),

is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 25 years, or both; and

(*b*) In the case of a body corporate, a fine not exceeding K1,000,000.00.

45. DISCLOSURE OF DETAILS OF AN INVESTIGATION.

An ICT Service Provider who is in receipt or has knowledge of a Court Order relating to an investigation or proceeding which explicitly stipulates that confidentiality is to be maintained or such obligation is required by law, intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification, or recklessly discloses -

(*a*) the fact that an order has been made; or

(*b*) anything done or required to be done under the order; or

(*c*) any data collected or recorded pursuant to that order,

is guilty of a crime.

Penalty: (*a*) In the case of a natural person, a fine not exceeding K100,000.00 or imprisonment for a term not exceeding 25 years, or both; and

(*b*) In the case of a body corporate, a fine not exceeding K500,000.00.

PART VI. - INTERNATIONAL CO-OPERATION.

46. MUTUAL ASSISTANCE.

For the purposes of facilitating international co-operation the provisions of the ***Mutual Assistance in Criminal Matters Act*** **2005** applies.

47. EXTRADITION.

For the purposes of facilitating matters relating to extradition, the provisions of the ***Extradition Act*** **2005** applies.

PART VII. - CERTAIN INDICTABLE OFFENCES, REGULATIONS, ETC.

48. INDICTABLE OFFENCES TRIABLE SUMMARILY.

Where a person is charged before a District Court constituted by a Principal Magistrate with an offence specified in Schedule 2, the Court may deal with the charge summarily according to the procedure set out in Section 421 of the ***Criminal Code Act*** (Chapter 262).

49. RULES, ETC.

Rules of any form of subordinate enactment necessary for the regulating of practice and procedure during an investigation or before a Court may be made prescribing all matters that are necessary or convenient to be prescribed for carrying out and giving effect to this Act, and in particular, for prescribing rules in relation to the provisions under Part IV.

50. REGULATIONS.

The Head of State, acting on advice, may make regulations, not inconsistent with this Act, prescribing all matters that, by this Act, are required or permitted to be prescribed, or that are necessary or convenient to be prescribed for carrying out or giving effect to this Act.

SCHEDULE 1.

DESCRIPTION OF ICT SERVICE PROVIDERS.

Sec. 1.

ICT SERVICE PROVIDERS	DESCRIPTION
Telecommunications Service Provider	means an ICT Service Provider that provides mobile or fixed line telephony services.
Internet Service Provider	means an ICT Service Provider that provides a service to connect users to the internet and to allow users to remain online by means which include, but are not limited to existing fixed lines, cable TV lines, fiber optic cables or by satellite.
Access Provider	means an ICT Service Provider providing an electronic communication transmission service by transmitting information provided by or to a user of the service in a communication network or providing access to a communication network.
Caching Provider	means an ICT Service Provider providing a dedicated network server or service acting as a server that saves Web pages or other internet content locally by placing previously requested information in temporary storage, or cache, a cache server both speeds up access to data and reduces demand on an enterprise's bandwidth.
Hyperlink Provider	means an ICT Service Provider providing a link from a hypertext document to another location.
Web Hosting Provider	means an ICT Service Provider providing an applications service whether shared, dedicated or virtual private server hosting, providing hosting services, which includes but is not limited to hosting services such as hosting files, images, games, webmail or similar content.
Website Master or Administrator	means a person responsible for maintaining one or many websites, also referred to as web architect, web developer, site author, website co-ordinator or website publisher.

SCHEDULE 2.

Sec. 44.

INDICTIBLE OFFENCES TRIABLE SUMMARILY.

CYBERCRIME CODE SECTIONS.	BRIEF DESCRIPTION OF OFFENCE.
6(1)	Unauthorised Access or Hacking.
8	Data Interference.
9(1)	Systems Interference.
11	Illegally Remaining.
14(1)	Electronic Gambling or Lottery by a Child.
15	Identity Theft.
21(2)	Defamatory Publication.
22(1), (2)	Cyber Bullying.
23(1), (2)	Cyber Harassment.
25(1)	Unlawful Disclosure.
26	Spam.
31	Unlawful Advertising.

I hereby certify that the above is a fair print of the ***Cybercrime Code Act* 2016** which has been made by the National Parliament.

Acting Clerk of the National Parliament.

13 DEC 2016

I hereby certify that the ***Cybercrime Code Act* 2016** was made by the National Parliament on 11 August 2016 by an absolute majority as required by the ***Constitution***.

Acting Speaker of the National Parliament.

13 DEC 2016