THIRD SUPPLEMENT TO THE GIBRALTAR GAZETTE

No. 3,726 of 23rd July, 2009

B. 24/09

CRIMES (COMPUTER HACKING) ACT 2009

ARRANGEMENT OF CLAUSES

Clauses.

THIRD SUPPLEMENT TO THE GIBRALTAR GAZETTE
No. 3,726 of 23rd July, 2009

B. 24/09

BILL

FOR

AN ACT to provide for the protection of computer systems and computer data from unauthorised access, use or modification; and for related purposes.

ENACTED by the Legislature of Gibraltar.

Title and commencement.

1. This Act may be cited as the Crimes (Computer Hacking) Act 2009 and comes into operation on the day of publication.

Interpretation.

2.(1) In this Act, unless the context otherwise requires–

"computer data" means a representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

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

"service provider" means–

(a) any public or private entity that provides to users of its service the ability to communicate by means of a computer system; and

(b) any other entity that processes or stores computer data on behalf of such communication service or users of such a service;

"traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer 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.

(2) For the purposes of this Act, a person secures access to any program or data held in a computer if by causing a computer to perform any function he–

(a) alters or erases the program or data;

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

(c) uses it; or

(d) has it output from the computer in which it is held (whether by having it displayed or in any other manner),

and references to access to a program or data (and to an intent to secure such access or to enable such access to be secured) are to be read accordingly.

(3) For the purposes of subsection (2)(c) a person uses a program if the function he causes the computer to perform–

(a) causes the program to be executed; or

(b) is itself a function of the program.

(4) For the purposes of subsection (2)(d)–

(a) a program is output if the instructions of which it consists are output; and

(b) the form in which any such instructions or any other data is output (and in particular whether or not it represents a form in which, in the case of instructions, they are capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial.

(5) For purposes of this Act, subject to subsection (7), access of any kind by any person to any program or data held in a computer is unauthorised if–

(a) he is not himself entitled to control access of the kind in question to the program or data; and

(b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.

(6) In this Act–

(a) references to any program or data held in a computer include references to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium;

(b) an act done in relation to a computer is unauthorised if the person doing the act (or causing it to be done)–

(i) is not himself a person who has responsibility for the computer and who is entitled to determine whether the act may be done; and

(ii) does not have consent to the act from any such person;

(c) "act" includes a series of acts;

(d) a reference to doing an act includes a reference to causing an act to be done;

(e) references to a program include references to part of a program.

Computer misuse offences

Unauthorised access to computer material.

3.(1) A person commits an offence if–

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer or to enable any such access to be secured;

(b) the access he intends to secure or to enable to be secured is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at–

(a) any particular program or data;

(b) a program or data of any particular kind; or

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

Unauthorised access with intent to commit or facilitate commission of further offences.

4.(1) A person commits an offence under this section if he commits an offence under section 3 with intent–

(a) to commit an offence to which this section applies ("the further offence"); or

(b) to facilitate the commission of such an offence (whether by himself or by any other person).

(2) This section applies to offences–

(a) for which the sentence is fixed by law; or

(b) for which a person of or over the age of 18 years may be sentenced to imprisonment for 5 years or more.

(3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the offence under section 3 or on any future occasion.

(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.

Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer etc.

5.(1) A person commits an offence if–

(a) he does any unauthorised act in relation to a computer;

(b) at the time when he does the act he knows that it is unauthorised; and

(c) either subsection (2) or (3) applies.

(2) This subsection applies if the person intends by doing the act–

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer;

(c) to impair the operation of any such program;

(d) to impair the reliability of any such data or the authenticity of any such data resulting in it being considered or acted upon for legal purposes as authentic;

(e) to cause a loss of property to any other person or to derive an economic benefit for himself or any other person; or

(f) to enable any of the things mentioned in paragraphs (a) to (e) to be done.

(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in subsection (2)(a) to (f).

(4) The intention referred to in subsection (2), or the recklessness referred to in subsection (3), need not relate to–

(a) any particular computer;

(b) any particular program or data; or

(c) a program or data of any particular kind.

(5) In this section–

(a) "impair" includes damaging a computer; deleting, deteriorating, altering or suppressing data; inputting data to cause damage, deterioration, alteration or suppression; and introducing contaminants to cause the cessation of a computer's functions; and

(b) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.

Unauthorised interception of computer service.

6.(1) A person commits an offence if–

(a) he does any unauthorised act in relation to a computer;

(b) at the time he does the act he knows that it is unauthorised; and

(c) he intends by doing the act to intercept or cause to be intercepted, directly or indirectly, any non-public electronic transmission or electro-magnetic emission of computer data to, from or within a computer, by any electro-magnetic, acoustic, mechanical or other technical means.

(2) The intention referred to in subsection (1)(c) need not relate to–

(a) any particular computer;

(b) any particular transmission or emission;

(c) any particular data; or

(d) a transmission or emission of any particular kind.

Making, supplying or obtaining articles for use in offence under section 3, 5 or 6.

7.(1) A person commits an offence if he makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 3, 5, or 6.

(2) A person commits an offence if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 3, 5 or 6.

(3) A person commits an offence if he obtains or possesses any article with a view to its being supplied for use to commit, or to assist in the commission of, an offence under section 3, 5 or 6.

(4) In this section "article" includes any program or data held in electronic form.

Unauthorised disclosure of access code.

8.(1) A person commits an offence if for any wrongful gain or unlawful purpose, and knowing that the access intended to be secured is unauthorised and is likely to cause wrongful loss to any person–

(a) he discloses any password, access code or any other means of gaining access to any program or data held in a computer;

(b) he possesses any password, access code or any other means of gaining access to any program or data in a computer with a view to its being used or supplied for use to commit, or to assist in the commission of an offence under section 3, 5 or 6.

(2) The intention referred to in subsection (1) need not relate to–

(a) any particular computer;

(b) any particular program or data; or

(c) a program or data of any particular kind.

Attempts and ancillary offences punishable as offences.

9.(1) A person who attempts to commit or who aids and abets the commission of or who does any act preparatory to or in furtherance of the commission of any offence under this Act commits that offence and is liable on conviction to the punishment provided for the offence.

(2) For an offence to be committed under this section, it is immaterial where the act in question took place.

Jurisdiction

Territorial scope of offences under this Act.

10.(1) Except as provided in this section, it is immaterial for the purposes of any offence under section 3 to 9–

(a) whether any act or other event proof of which is required for conviction of the offence occurred in Gibraltar; or

(b) whether the accused was in Gibraltar at the time of any such act or event.

(2) Subject to subsection (3), in the case of such an offence at least one significant link with Gibraltar must exist in the circumstances of the case for the offence to be committed.

(3) There is no need for any such link to exist for the commission of an offence under section 3 to be established in proof of an allegation to that effect in proceedings for an offence under section 4.

(4) Subject to section 13, if–

(a) any such link does in fact exist in the case of an offence under section 3; and

(b) commission of that offence is alleged in proceedings for an offence under section 4,

section 4 applies as if anything the accused intended to do or facilitate in any place outside Gibraltar which would be an offence to which section 4 applies if it took place in Gibraltar were the offence in question.

Significant links with Gibraltar.

11.(1) The following provisions of this section apply for the interpretation of section 10.

(2) In relation to an offence under section 3, either of the following is a significant link with Gibraltar–

(a) that the accused was in Gibraltar at the time when he did the act which caused the computer to perform the function; or

(b) that any computer containing any program or data to which the accused by doing that act secured or intended to secure unauthorised access, or enabled or intended to enable unauthorised access to be secured, was in Gibraltar at that time.

(3) In relation to an offence under section 5 or 6, either of the following is a significant link with Gibraltar–

(a) that the accused was in Gibraltar at the time when he did the unauthorised act (or caused it to be done); or

(b) that the unauthorised act was done in relation to a computer in Gibraltar.

Territorial scope of inchoate offences related to offences under this Act.

12.(1) On a charge of conspiracy to commit an offence under this Act the following questions are immaterial to the accused's guilt–

(a) where any person became a party to the conspiracy; and

(b) whether any act, omission or other event occurred in Gibraltar.

(2) On a charge of attempting to commit an offence under section 5 or 6 the following questions are immaterial to the accused's guilt–

(a) where the attempt was made; and

(b) whether it had an effect in Gibraltar.

(3) On a charge of incitement to commit an offence under section 3 to 9, the question where the incitement took place is immaterial to the accused's guilt.

Relevance of external law.

13.(1) A person commits an offence triable by virtue of section 10(4) only if what he intended to do or facilitate would involve the commission of an offence under the law in force where the whole or any part of it was intended to take place.

(2) A person commits an offence triable by virtue of section 12 only if what he had in view would involve the commission of an offence under the law in force where the whole or any part of it was intended to take place.

(3) Conduct punishable under the law in force in any place is an offence under that law for the purposes of this section, however it is described in that law.

(4) Subject to subsection (6), a condition specified in subsection (1) or (2) is to be taken as satisfied unless, not later than rules of court may provide, the defence serve on the prosecution a notice–

(a) stating that, on the facts as alleged with respect to the relevant conduct, the condition is not in their opinion satisfied;

(b) showing their grounds for that opinion; and

(c) requiring the prosecution to show that it is satisfied.

(5) In subsection (4) "the relevant conduct" means–

(a) if the condition in subsection (1) is in question, what the accused intended to do or facilitate;

(b) if the condition in subsection (2) is in question, what the accused had in view.

(6) The court, if it thinks fit, may permit the defence to require the prosecution to show that the condition is satisfied without the prior service of a notice under subsection (4).

(7) In the Supreme Court the question whether the condition is satisfied is to be decided by the judge alone.

National status immaterial.

14.(1) In any proceedings brought in respect of any offence to which this section applies it is immaterial to guilt whether or not the accused was a Gibraltarian at the time of any act, omission or other event proof of which is required for conviction of the offence.

(2) This section applies to the following offences–

(a) any offence under section 3 to 9;

(b) any attempt to commit an offence under section 5 or 6; and

(c) incitement to commit an offence under section 3 to 9.

(3) For the purposes of this section "Gibraltarian" has the meaning given to it by the Gibraltarian Status Act.

Investigation of offences

Search warrants for offences under this Act.

15.(1) If a magistrate is satisfied by information on oath given by a police officer that there are reasonable grounds to suspect–

(a) that an offence under this Act has been or is about to be committed in any premises; and

(b) that evidence that such an offence has been or is about to be committed is in those premises,

the magistrate may issue a warrant authorising a police officer to enter and search the premises, using such reasonable force as is necessary.

(2) A warrant under this section–

(a) may authorise persons with appropriate technical knowledge and expertise to accompany and assist, as necessary, the police officer executing the warrant; and

(b) remains in force for as long as is reasonably necessary for the investigation of an offence.

(3) In executing a warrant issued under this section a police officer may seize an article if he reasonably believes that it is evidence that an offence under this Act has been or is about to be committed or that the article has been acquired by a person as a result of an offence committed under this Act.

(4) In seizing any article referred to in subsection (3), a police officer must have due regard to the rights and interests of any person affected by such seizure to carry on his normal activities.

(5) A person who without lawful excuse obstructs the lawful exercise of the powers granted under this section commits an offence.

(6) In this section–

"premises" includes land, buildings, movable structures, vehicles, vessels, aircraft and hovercraft;

"article" includes a computer or part of a computer, a computer system or part of it, a computer data storage system and a document.

Warrant for access to computer and data for investigation of offences under this Act.

16.(1) If a magistrate is satisfied by information on oath given by a police officer that there are reasonable grounds to suspect–

(a) that a computer is being or has been used in connection with an offence under this Act; and

(b) that evidence that such an offence is being or has been committed is in that computer,

the magistrate may issue a warrant authorising a police officer to do such things as are permitted under subsection (2).

(2) A warrant under subsection (1) may authorise a police officer to enter any premises where the computer is kept, using such reasonable force as is necessary, and to–

(a) have access to and use the computer and examine the operation of that computer;

(b) search any data stored or available in the computer or in any computer data storage system forming part of the computer; or

(c) have access to any password or access code or any other means of gaining access to the computer;

(d) have access to any program having the capability of retransforming or unscrambling encrypted data in the computer into readable and comprehensible format or into plain text;

(e) make and take any copies or take any samples of any data held in the computer; and

(f) require any person whom the police officer has reasonable cause to suspect is or has been using the computer, or any person having charge or control of or operating the computer, to provide him with such reasonable technical and other assistance as he may require for the purposes of carrying out the investigation authorised under this section.

(3) In taking any samples or copies of data or performing any of the actions referred to in subsection (2), a police officer must have due regard to the rights and interests of any person affected by such actions to carry on his normal activities.

(4) A warrant under this section–

(a) may authorise persons with appropriate technical knowledge and expertise to accompany and assist, as may be necessary, a police officer executing the warrant; and

(b) remains in force until such time as may be reasonably be required for the investigation of an offence.

(5) A person who without lawful excuse obstructs the lawful exercise of the powers under subsection (2)(a) to (e) or who fails to comply with a requirement under subsection (2)(f) commits an offence.

(6) An information given under subsection (1) may be combined with an information given for the purposes of section 15 and a warrant issued under this section may be combined with a warrant issued under that section.

(7) In this section "premises" has the meaning given by section 15(6).

Record of seized articles, etc.

17.(1) If a computer or computer program or data has been removed following a search under section 15, the police officer who carried out the search must, at the time of the search or as soon as practicable after it–

(a) make an official record of the articles seized and removed, of the premises from where they were removed, and the date and time of seizure; and

(b) give a copy of the record to the owner, lessee or occupier of the premises if they are immovable property; to the master, captain or person in charge of a vehicle, vessel, aircraft, hovercraft or other movable structure; or to the person in charge or control of the articles seized and removed.

(2) Subject to subsection (3), if a computer has been used or its operation examined or a program or data has been accessed under section 16, the police officer who carried out those actions may authorise a person who had charge or control of the computer to access and copy a program or data in the computer.

(3) The police officer may refuse to permit access to the computer under subsection (2) if he has reasonable grounds for believing that giving the access would lead to the commission of a criminal offence or would prejudice–

(a) the investigation in connection with which the search was carried out;

(b) another ongoing investigation; or

(c) any criminal proceedings which are pending or which may be brought in relation to any of those investigations.

Preservation of data.

18.(1) If the Commissioner of Police is satisfied that–

(a) a program or data, including traffic data, stored in a computer is necessary for the purposes of a criminal investigation; and

(b) there is a risk that the program or data may be lost, destroyed or rendered inaccessible or modified,

he may by written notice given to a person in charge or in control of the computer require that person to ensure that the program or data specified in the notice be preserved for as long as is reasonably necessary for the investigation of an offence.

(2) Traffic data may be ordered to be preserved under subsection (1) irrespective of whether one or more service providers were involved in the transmission of the data.

(3) A person who without lawful excuse fails to comply with a requirement under this section commits an offence.

Interception of traffic data.

19.(1) If the Commissioner of Police is satisfied that traffic data associated with a specified communication or general traffic data is reasonably required for the purposes of a criminal investigation, he may, by written notice given to a person in charge or in control of such data or to an internet service provider, require that person or service provider to–

(a) collect and record traffic data associated with such communication for the period of time specified in the notice; or

(b) permit and assist any named person with appropriate technical knowledge and expertise to collect and record that data.

(2) A person who without lawful excuse fails to comply with a requirement under this section commits an offence.

Order for disclosure of stored traffic.

20.(1) If a magistrate is satisfied on an application by a police officer that specified data stored in a computer is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may issue an order requiring a person in charge or in control of the computer to preserve and disclose to a police officer an amount of traffic data about specified communication sufficient to identify–

(a) the internet service providers; and

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

(2) A person who without lawful excuse fails to comply with a requirement under this section commits an offence.

Order for production of data.

21.(1) If a magistrate is satisfied on an application by a police officer that a specified computer program, data, printout of that data or any other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may issue an order requiring–

(a) a person in charge or in control of a computer to produce to a police officer any computer program, data or printout of data specified in the order which is stored in the computer or in a computer data storage system in that person's possession or control; and

(b) an internet service provider with a place of business in Gibraltar to produce to a police officer any subscriber information specified in the order relating to a service provided by that service provider.

(2) In this section, "subscriber information" means any information in the form of computer data, or in any other form, which is held by a service

provider, which relates to subscribers of its service other than traffic or content data, and by which can be established–

(a) the subscriber's identity, telephone or access number, postal address and billing and payment information;

(b) the type of communication service used by the subscriber, the technical provisions relating to it and the period of service; and

(c) any other information on the site relating to the installation of communication equipment.

(3) A person who without lawful excuse fails to comply with a requirement under this section commits an offence.

Order for interception of electronic communication.

22.(1) If a magistrate is satisfied on an application by a police officer that the contents of electronic communication or any other information connected with such communication are reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may issue an order requiring an internet service provider with a place of business in Gibraltar–

(a) to apply such technical means as are necessary to collect and record; or

(b) to permit or assist any named person with appropriate technical knowledge and expertise to collect and record,

content data associated with specified communications transmitted by means of a computer.

(2) A person who without lawful excuse fails to comply with a requirement under this section commits an offence.

Rights and duties of internet service providers.

23.(1) An internet service provider is not liable under civil or criminal law for the disclosure of any data or other information that he discloses under any of sections 19 to 22.

(2) An internet service provider who without lawful authority discloses–

(a) the fact that a notice has been given under section 19 or that an order has been issued under section 20, 21 or 22;

(b) anything done under the notice or order; or

(c) any data collected or recorded under the notice or order,

commits an offence.

Saving for certain law enforcement powers.

24.(1) Section 3(1) does not affect the operation of other provisions of this Act or any other enactment relating to powers of inspection, search or seizure.

(2) Nothing designed to indicate a withholding of consent to access to any program or data from persons as enforcement officers makes access unauthorised for the purposes of section 3(1).

(3) In subsection (2)–

(a) "enforcement officer" means a police officer or other person charged with the duty of investigating offences; and

(b) withholding consent from a person "as" an enforcement officer of any description includes the operation, by the person entitled to control access, of rules whereby enforcement officers of that description are, as such, disqualified from membership of a class of persons who are authorised to have access.

Penalties.

25.(1) A person who commits an offence under section 3, 7 or 8 is liable–

(a) on summary conviction to imprisonment for 6 months or the statutory maximum fine, or both;

(b) on conviction on indictment to imprisonment for 2 years.

(2) A person who commits an offence under section 4 or 6 is liable–

(a) on summary conviction to imprisonment for 6 months or the statutory maximum fine, or both;

(b) on conviction on indictment to imprisonment for 5 years.

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

(a) on summary conviction to imprisonment for 12 months or the statutory maximum fine, or both;

(b) on conviction on indictment to imprisonment for 10 years.

(4) A person or a service provider who commits an offence under section 14, 16, 18, 19, 20, 21, 22, 23 or 29 is liable on summary conviction to the statutory maximum fine.

Offences by and for the benefit of corporate bodies.

26.(1) If an offence under section 3, 4, 5 or 6 which was committed by any person is proved to have been committed for the benefit of a corporate body, irrespective of whether that person acted individually or as the holder of a position in or as the agent of the corporate body, the corporate body commits a similar offence.

(2) A corporate body which commits an offence under subsection (1) is liable on summary conviction to twice the statutory maximum fine.

(3) If an offence under this Act is committed by a corporate body and it is proved–

(a) to have been committed with the consent or connivance of an officer; or

(b) to be attributable to any neglect on the part of an officer,

the officer as well as the corporate body commits the offence and is liable to be proceeded against and punished accordingly.

(4) In subsection (1) "officer", in relation to a corporate body, means a director, manager, secretary or other similar officer of the body, or a person purporting to act in any such capacity.

(5) If the affairs of a corporate body are managed by its members, subsection (3) applies in relation to the acts and defaults of a member in connection with his functions of management as if he were a director of the body.

Forfeiture.

27. A court before which a person is convicted of an offence under any of sections 3 to 9 may, in addition to imposing any other penalty, make an order for the forfeiture of any computer, computer program or data, computer data storage system, or other apparatus, article or thing which is the subject matter of the offence or which was used in connection with the commission of the offence.

Compensation.

28.(1) The court before which a person is convicted of an offence under any of sections 3 to 9 may order the person to pay a sum fixed by the court by way of compensation to any other person for damage caused to that person's computer, computer data storage system, program or data by the offence for which the person is convicted.

(2) A claim by a person for damage caused by an offence under any of section 3 to 9 is deemed to have been satisfied to the extent of any amount ordered to be paid to him by way of compensation under subsection (1), but the order does not affect any right to a civil remedy for the recovery of damages beyond the amount of such compensation.

(3) Compensation awarded by an order under subsection (1) is recoverable as a civil debt.

Breach of confidentiality.

29.(1) Except for any prosecution for an offence under this Act, for other purposes of this Act, or for or pursuant to an order of a court, a person who has had access to–

(a) any computer, computer data storage system, program or data during the course of an investigation under this Act;

(b) any record, book, register, correspondence, information, document or any other material during the course of an investigation under this Act;

(c) any confidential information which may have been received from the competent authorities of a State which is a party to the Convention, for the purpose of an investigation under this Act,

must not disclose to any other person, or use for any purpose other than that for which he obtained access or received information, the contents of the material mentioned in paragraphs (a) to (c).

(2) A person who contravenes subsection (1) commits an offence.

(3) In subsection (1) "the Convention" means the Council of Europe Convention on Cybercrime of 23 November 2001.

EXPLANATORY MEMORANDUM

This Act criminalises the various forms of computer abuse, unauthorised access to computer data and other attacks against information systems The Act also transposes, in part, into the law of Gibraltar Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems and implements the 2001 Council of Europe Convention on Cybercrime.

Clause 3 makes it an offence for a person knowingly to have unauthorized access to any program or data held in a computer. Clause 4 makes it an offence for a person to access a computer program or data with intent to commit or facilitate the commission of another offence for which the sentence is fixed by law or a sentence of at least 5 years imprisonment.

Clause 5 makes it an offence for a person to do an act, whether temporary or permanent, which he knows will cause an impairment of the operation of a computer or any program or data held in a computer or an impairment of the reliability or the authenticity of any such data. Clause 6 makes it an offence

for a person knowingly to intercept any non-public transmission from a computer without authority.

Clause 7 makes it an offence for any person to produce, sell or procure for use any device, program or data which is designed or adapted with the intention that it should be used to commit any other offence under the Act.

Clause 8 makes it an offence for any person, knowingly and without authority, to disclose any password or access code of a computer that is capable of being accessed, with the intention that it be used by any person for the purpose of committing an offence.

Clause 9 punishes as an offence any aiding and abetting of the commission of any other offence under the Act.

Clauses 10 to 14 provide for the territorial scope of offences under the Act. It is irrelevant whether the offender is a Gibraltarian, provided he or the computer was in Gibraltar at the material time.

Clause 15 empowers a magistrate to issue a search warrant to a police officer, who, upon executing it, may seize any computer or computer program or data if he believes it is evidence that an offence has been committed or is about to be committed.

Clause 16 allows a police office to have access to any computer, or any program or data held in any computer, and to require any person concerned to assist him in his investigations. Clause 17 requires the police officer to make and deliver to the person in charge of a computer a record of the seized articles.

Clauses 18 and 19 enable the Commissioner of Police to require the preservation of data if data stored in a computer is required for the purposes of a criminal investigation; and if there is a risk that the data may be destroyed or rendered inaccessible or modified.

Clauses 20, 21 and 22 empower the Magistrates' Court to order production of data required for the purpose of a criminal investigation or criminal proceedings; to authorise a police officer to collect or record traffic data associated with a specified communication during a specified period if there are reasonable grounds to suspect that traffic data is required for the purposes of a criminal investigation; and to order internet service providers

to intercept electronic communications and data traffic where necessary for criminal investigations.

Clause 23 makes it an offence for an internet provider to disclose the fact that the powers under clauses 19 to 22 have been used, or any information given by the provider in response to a notice or order under those powers. An internet provider is not liable for the disclosure of any information given in response to such a notice or order.

Clause 24 gives law enforcement officers the powers of inspection, search and seizure notwithstanding the requirement for consent under clause 3(1).

Clause 25 prescribes the penalties for offences by way of terms of imprisonment and fines. It makes the offences triable both ways by prescribing both indictable and summary penalties. The summary penalty is set at 12 months for the offences which carry an indictable penalty of 10 years imprisonment. It is at 6 months or the statutory maximum fine for other indictable offences, and at the statutory maximum fine for other offences.

Clause 26 makes it an offence for a corporate body to benefit from the commission of an offence under clauses 3 to 6, whether or not the person was acting as an agent of the body. It also provides that officers of the company may incur personal liability in addition to that incurred by the corporate body.

Clause 27 empowers a court to order the forfeiture of a computer and other articles used in connection with an offence. Clause 28 enables a court to make an order for payment of compensation by the offender to any person for damage caused to that person's computer or any program or data held in his computer.

Clause 29 creates an offence of unauthorised disclosure of information obtained during the course of an investigation or of information received from the competent authorities of a Party to the Convention for the purposes of or to assist in the investigation of offences.

Printed by the Gibraltar Chronicle Limited
Printing Office, 2, Library Gardens,
Government Printers for Gibraltar,
Copies may be purchased at 6, Convent Place, Price £1.45p