STATES OF JERSEY

DRAFT CYBERCRIME (JERSEY) LAW 201-

Lodged au Greffe on 29th October 2018
by the Minister for Home Affairs

STATES GREFFE

DRAFT CYBERCRIME (JERSEY) LAW 201-

European Convention on Human Rights

In accordance with the provisions of Article 16 of the Human Rights (Jersey) Law 2000, the Minister for Home Affairs has made the following statement –

In the view of the Minister for Home Affairs, the provisions of the Draft Cybercrime (Jersey) Law 201- are compatible with the Convention Rights.

Signed: **Connétable L. Norman of St. Clement**

Minister for Home Affairs

Dated: 15th October 2018

REPORT

Introduction

The Draft Cybercrime (Jersey) Law 201- ("draft Law") will bring Jersey up-to-date in its treatment of crime involving computers and data storage. The draft Law is a series of amendments to other legislation, which together will provide authorities with sufficient powers to deal with increasingly sophisticated online criminal activity, and will make Jersey compliant with the international treaties in this area.

When it is in place, we will be in a position to have the Council of Europe Convention on Cybercrime (the Budapest Convention) extended to the Island. The Convention is concerned with crimes committed over the Internet, particularly infringements of copyright, computer-related fraud, child pornography, hate crimes, and violations of network security. It contains a series of powers and procedures such as the search of computer networks and lawful interception, and also requires legal controls on the dissemination of racist and xenophobic material and threats through computer systems.

Like any convention, the act of ratification does not provide additional powers to the countries concerned, but as signatories must have committed to a common legal framework to enter the treaty arrangements, the potential for international co-operation is greatly enhanced.

Principles

Currently, access to physical information held by an individual is available by a search warrant granted by a court. This could include financial records, itemised telephone bills, personal diaries, etc. Broadly speaking, the draft Law will allow access to information held on computer systems on the same terms, with the same safeguards.

The draft Law is required in order to keep pace with developments in the use of technology: as more data is stored electronically, there is a growing realisation that e-crime is simply another form of crime, and e-data is simply evidence held in a novel manner.

Law enforcement

The draft Law will provide for additional powers, addressed in detail below, where computer systems are used to commit offences or hide evidence of offences. Amongst other things, these will strengthen Jersey's capacity to charge and prosecute people for possessing, making or distributing indecent images of children. In addition, Jersey's ability to provide assistance to other jurisdictions will be improved.

The draft Law will also serve to bring certain offences regarding computer misuse into line with equivalent offences in the United Kingdom; and to give greater powers to law enforcement authorities to access devices which are password-protected or locked by other means, in line with the UK's Regulation of Investigatory Powers Act 2000. This will improve our domestic response to criminal activity, as well as satisfy certain parts of the Convention.

This report is intended to address the key elements of the Law, and specific legal detail can be found in the Explanatory Note which follows the report.

International compliance

Jersey's compliance with international standards against money laundering and terrorist financing is overseen by the 'Committee of Experts on the Evaluation of

Anti-Money Laundering Measures and the Financing of Terrorism'. Generally referred to as MONEYVAL, this is an independent monitoring mechanism within the Council of Europe, which reports to the Committee of Ministers on members' compliance with relevant international standards.

The most recent report on Jersey was conducted in 2015, and noted that Jersey had both well-functioning anti-money laundering and counter-terrorist financing processes, as well as a proactive approach to international co-operation. However, it was noted that the Budapest Convention had not been extended to Jersey, with the expectation that this would be achieved as soon as possible.

The amendments

The draft Law consists of amendments to the following pieces of legislation –

- Computer Misuse (Jersey) Law 1995
- Criminal Justice (International Co-operation) (Jersey) Law 2001
- Police Procedures and Criminal Evidence (Jersey) Law 2003
- Regulation of Investigatory Powers (Jersey) Law 2005.

Computer Misuse (Jersey) Law 1995 ("CML")

The CML is to be amended to bring it more into line with its UK equivalent, the modernised Computer Misuse Act 1990. The specific changes are –

- *Article 2: Unauthorised access to computer material ('hacking')*

Article 2 provides that it is an offence to knowingly use a computer with intent to secure unauthorised access to any programme or data. The current maximum penalty is 6 months and/or a fine. This is to be widened to match the UK Act to also include enabling unauthorised access and the penalty increased to 2 years' imprisonment and/or a fine.

'Enabling' unauthorised access to computer material could mean providing an unauthorized person with a password, or by hacking into a system for someone.

- *Article 5: Unauthorised modification of computer material*

The Convention requires parties to adopt legislation to criminalise the intentional and unauthorised damaging, deterioration, alteration or suppression of computer data, as well as measures to establish as criminal offences the intentional and unauthorised inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing of computer data.

The offence in Article 5 currently concerns the unauthorised modification of the contents of any computer. The scope of the Convention is wider than 'modification' captures, so that term is removed, and the offence becomes knowingly or recklessly doing 'any unauthorized act' (as defined in the Law) to cause impairment to any computer, hinder access to programs or data, or impair the operation of a program or reliability of data (sabotage). This will be in line with the UK position, and would be punishable by a maximum sentence of 10 years' imprisonment and/or a fine.

For example, a person could impair a computer by damaging the computer database of a competitor, and a person could prevent or hinder access to incriminating data to try and avoid prosecution.

- *New Article 5A: Making, supplying or obtaining articles for use in other offences*

The Convention requires signatories to criminalise the production, ownership, use and movement of various devices designed or adapted to commit offences such as accessing or intercepting data.

Article 5A creates an offence of making, adapting, supplying such items, and is modelled on section 3A of the UK Act. The maximum penalty will be 2 years' imprisonment and/or a fine.

This offence is intended to cover persons who provide others with devices which cause unauthorised access to computer material or unauthorised acts which impair or damage computer material. An example might be a person who supplies a device which can hinder access to or damages a computer device held by the police who are investigating the contents of it.

Criminal Justice (International Co-operation) (Jersey) Law 2001 ("CJICL")

The CJICL is concerned with the provision of mutual legal assistance between jurisdictions, which is a core aim of the Convention.

Article 29 of the Convention requires parties to take the appropriate measures to preserve data at the request of another state party, in the expectation that a formal request for mutual legal assistance will be received.

New Article 5C of the CJICL will make the necessary provisions for the Court, on the application of the Attorney General, to order the preservation of data as a preliminary measure before the requesting country gathers the necessary evidence to make a formal request for mutual legal assistance.

The penalty for contravention of a preservation order would be up to 5 years' imprisonment and/or a fine.

For example, in a drug trafficking case, text messages sent to and from a phone number may serve as crucial evidence, and it will be in the interests of the authorities to make an order on the telecommunications provider requiring that such data is preserved before a request for mutual legal aid is made.

Police Procedures and Criminal Evidence (Jersey) Law 2003 ("PPCE")

The Convention requires that parties empower the competent authorities to order persons or service providers to submit specified computer data or subscriber information that they possess or control.

- *The current position under PPCE*

There are 2 types of material that have significant additional protections, called 'excluded material' and 'special procedure material'.

Excluded material includes confidential personal records created in the course of any occupation or for the purposes of any office, as well as human tissue or fluids held for medical purposes, and journalistic material held in confidence.

Special procedure material means personal records created in the course of any occupation or for the purposes of any office, where held under an undertaking of confidence, and journalistic material other than that 'excluded' above.

Article 16 of PPCE currently provides that a police officer may make an application to the Bailiff under Schedule 2 of PPCE about excluded and special procedure material,

which requires a person who appears to be in possession of such material to either produce the material to a police officer or give a police officer access. The Bailiff may also issue an ancillary entry and search warrant allowing a police officer to seize and retain items.

- *Amended Article 16 and Schedule 2*

In order to achieve compliance with the Convention, Article 16 of PPCE would be widened so that in addition to excluded material and special procedure material, a police officer may obtain access to material stored on a computer or on a remote "cloud based" storage programme.

Schedule 2 would be amended to cover material in a person's control in addition to that in a person's possession, and there is also an allowance for the fact that material might not always be "on premises.".

Using these powers, a police officer might obtain an order requiring a person to give access to material stored on a computer which may be evidence for an investigation. The order can be wide enough to cover material stored on a cloud based programme.

This will not have any effect on the level of protection over such material, but will recognise the possibility that it might be held in electronic form.

- *New Articles 70A and 70B – preservation and tipping off*

As with the CJICL, to achieve Convention compliance, preservation orders are also introduced by new Article 70A into PPCE to allow them to be utilized for domestic criminal investigations. This would permit law enforcement authorities to efficiently preserve such data without having to go down the seizure route immediately.

A 'tipping off' offence would also be introduced by Article 70B, preventing disclosure of the existence or details of a preservation order in case this causes another person to take evasive steps. The maximum penalty for breaching this offence would be 5 years' imprisonment and/or a fine. This is intended to comply with Article 20 of the Convention, which is addressed below.

Regulation of Investigatory Powers (Jersey) Law 2005 ("RIPL")

- *Tipping off provision*

Where a party uses its power to compel a service provider by notice to collect or record traffic data, Article 20 of the Convention requires parties to adopt measures to oblige the service providers to keep that confidential.

Article 26 RIPL currently allows public authorities to require a postal or telecommunications operator to disclose data in its possession, or obtain and disclose data where it can. However, there is no provision preventing an operator from "tipping off" anyone about the service of such a notice. The new Article 27A would provide that it is an offence to fail to keep secret the existence and contents of such a notice. The penalty would be a maximum sentence of 5 years' imprisonment and/or a fine.

This new provision is broadly similar to an existing provision in Article 23 RIPL regarding the unauthorised disclosure of interception warrants.

- *Investigation of encrypted data*

Article 19 of the Convention requires authorities to have the ability to order an appropriate person to enable access to a computer system or storage by providing the necessary information about the functioning or security measures (e.g. a password) to access a computer, even if they do not have access to the system it unlocks.

This is also desirable for the law enforcement authorities in Jersey, as it will enable the States of Jersey Police, for example, to be able to require a person to grant them access to a device which is otherwise locked. To that end, Article 42B and Schedule 2A would empower a person (e.g. a police officer) with appropriate permission from the Bailiff, to issue a notice requiring the disclosure of information protected by a key (a password, key, code, algorithm, or biometric identification).

Such notice may be given only on the grounds of national security, for preventing or detecting crime, in the economic interests of Jersey, or to perform a statutory power or duty. It must be proportionate to what is sought to be achieved, and used only where the information cannot be acquired in any other way.

Knowingly failing to make a disclosure in accordance with such a notice carries a maximum penalty of 5 years' imprisonment and/or a fine.

Consultation history

The draft Law has been developed by a working group comprised of representatives from the Home Affairs Department/ Community and Constitutional Affairs Department, the Ministry for External Affairs, the Law Officers' Department, the States of Jersey Police and the Legislative Drafting Office.

The Bailiff, Deputy Bailiff and Attorney General have also been consulted on the contents of the draft Law, given the aspects which affect law enforcement and the courts.

Timetable for implementation

The Law will come into force 7 days after its registration.

Financial and manpower implications

There are no additional financial or resource implications for the States arising from the adoption of this draft Law.

Human Rights

The notes on the human rights aspects of the draft Law in the **Appendix** have been prepared by the Law Officers' Department and are included for the information of States Members. They are not, and should not be taken as, legal advice.

APPENDIX TO REPORT

Human Rights Notes on the Draft Cybercrime (Jersey) Law 201-

These Notes have been prepared in respect of the Draft Cybercrime (Jersey) Law 201- (the "**draft Law**") by the Law Officers' Department. They summarise the principal human rights issues arising from the contents of the draft Law and explain why, in the Law Officers' opinion, the draft Law is compatible with the European Convention on Human Rights ("**ECHR**").

These notes are included for the information of States Members. They are not, and should not be taken as, legal advice.

The draft Law will make amendments to Jersey criminal legislation to give further effect to the Council of Europe Convention on Cybercrime (Budapest, 2001) and amend the Regulation of Investigatory Powers (Jersey) Law 2005 to provide for the investigation of electronic data protected by encryption.

The draft Law engages several articles of the ECHR, which are addressed in turn.

Article 8 ECHR

1. Article 8 ECHR provides that –

   (a) Everyone has the right to respect for his private and family life, his home and his correspondence.

   (b) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

2. The draft Law engages Article 8 ECHR to the extent that the exercise of some of the powers, in particular the access powers in PPCE and the power in RIPL to require disclosure of protected information, may involve interference with a person's private or family life, or correspondence.

3. However, the second paragraph of Article 8 ECHR provides that such interference may be justifiable if the following criteria are met –

   (a) In accordance with the law: the interferences will be clearly prescribed in primary legislation and therefore this criterion is satisfied.

   (b) In pursuit of a legitimate aim: the second paragraph of Article 8 provides several legitimate aims which can justify interference with Article 8. The interest of national security, public safety, economic wellbeing of Jersey and the prevention of disorder or crime will all be applicable in this case.

   (c) Necessary in a democratic society: this final strand of compliance with a qualified ECHR right is concerned with whether or not the means being deployed are proportionate to the legitimate aim sought. It is submitted that the new powers are moderate and reasonable and

when weighed against the aims they seek to achieve, can be considered proportionate. Furthermore, there are several safeguards which ensure the powers are mitigated and used appropriately, such as the involvement of the judiciary, the requirements for notices to be made in writing and detailed and for the States to make necessary arrangements for appropriate contributions towards costs incurred by persons complying with disclosure notices, the duties on those who obtain possession of keys and the provision for loss or damage incurred by any breach or contravention of a person with appropriate permission.

4. Based on the above reasoning, the draft Law is compatible with Article 8 ECHR.

Article 10 ECHR

5. Article 10 provides that –

"Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers …"

6. New Article 27A RIPL and Article 70B PPCE will place a restriction on the ability of persons to make disclosures and "tip off" others, thus affecting the rights of persons to receive and impart information.

7. However, Article 10 is also a qualified right, and the interferences will be in accordance with law and may be justified on the grounds of one or more legitimate aims (set out in Article 10(2) ECHR) similar to Article 8 as described above.

8. As to proportionality, the new provisions are not radical and follow the precedent already established in Article 23 RIPL. Procedural safeguards for this restriction include the ability for a disclosure by or to a professional legal adviser, unless with a view to furthering a criminal purpose. Disclosures can also be made to the Information Commissioner or be authorised by the Commissioner, by the terms of the notice, by or on behalf of the person who gave the notice, or by or on behalf of a person who is in lawful possession of the protected information and came into possession of it. On balance therefore, the interference with the Article 10 right to impart and receive information is proportionate.

9. Based on the above reasoning, the draft Law is compatible with Article 10 ECHR.

Article 1, Protocol 1 ECHR ("A1, P1")

10. Article 1, Protocol 1 of the ECHR provides that –

"Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.

The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties."

11. The draft Law potentially engages A1, P1 to the extent that the peaceful enjoyment of property is interfered with by preservation orders, access to material, and requirements for disclosure of protected information. A1, P1 is also a qualified right and for the same reasons as expressed above regarding Article 8, the interferences by the draft Law with A1, P1 can be considered proportionate, particularly as the interferences will only amount to a control (and not a deprivation) of property.

12. Based on the reasoning above, the draft Law is compatible with A1, P1 ECHR.

Explanatory Note

This draft Law would make amendments to criminal legislation to give further effect to the Council of Europe Convention on Cybercrime (Budapest, 2001) and amend the Regulation of Investigatory Powers (Jersey) Law 2005 to provide for the investigation of electronic data protected by encryption.

Computer Misuse (Jersey) Law 1995 ("1995 Law")

Article 1(2) would amend the interpretation Article of the 1995 Law to widen it to cover unauthorized acts in relation to a computer rather than just the modification of its contents, these changes being a consequence of the changes to Article 5 of the 1995 Law. A power is added to enable further amendment of definitions to be done by Regulations.

Article 1(3) would amend Article 2 of the 1995 Law to make it an offence to enable the securing of unauthorized access to a computer and increase the penalty to imprisonment for up to 2 years and/or an unlimited fine.

Article 1(4) would amend the offence in Article 5 of the 1995 Law to make it an offence to do any unauthorized act in relation to a computer without the additional need for there to be a modification of the computer. The person concerned must have known it was unauthorized at the time and must either intend to impair or hinder access or be reckless as to doing so. The offence is to carry a sentence of up to 10 years' imprisonment and/or an unlimited fine. A new offence is created by the inserted Article 5A of making, supplying or obtaining articles for use in an offence under Article 2 or 5, which carries imprisonment for up to 2 years and/or an unlimited fine.

Criminal Justice (International Co-operation) (Jersey) Law 2001 ("2001 Law")

Article 2 would insert new Article 5C into the 2001 Law which enables the court to make an order preserving certain data specified in the application to be preserved pending the submission of a request for mutual legal assistance. It also inserts a new Article 5D to prevent anyone from "tipping off" another person in respect of preservation orders. This new offence is to carry up to 5 years' imprisonment and/or an unlimited fine.

Police Procedures and Criminal Evidence (Jersey) Law 2003 ("2003 Law")

Article 3(2) would substitute a new Article 16 of the 2003 Law widened to enable a police officer to obtain access to material stored on a computer or stored on the Internet.

Article 3(3) would insert a new Article 70A into the 2003 Law providing for preservation orders similar to those to be provided for in the 2001 Law. It also inserts a new Article 70B to prevent anyone from "tipping off" another person in respect of preservation orders. This new offence is to carry up to 5 years' imprisonment and/or an unlimited fine.

Article 3(4) makes changes to Schedule 2 to the 2003 Law consequential on the amendments to Article 16.

Regulation of Investigatory Powers (Jersey) Law 2005 ("2005 Law")

Article 4(2) would insert a new Article 27A into the 2005 Law to prevent a service provider from "tipping off" anyone as regards notices under Article 26 of the 2005 Law or information relating to them, equivalent to Article 23 of that Law. The new offence is to carry up to 5 years' imprisonment and/or an unlimited fine.

The other provisions in *Article 4* relate to the investigation of electronic data by encryption. *Paragraph (3)* would insert Part 3A, conferring powers where information in the format of electronic data that cannot be readily accessed or put into intelligible form ("protected information") lawfully comes into the possession of a person. The power conferred is to require another person to use a password or other means of decrypting the protected information (a "key") to render the information into intelligible form or to require a person who has the key, but not the protected information, to disclose the key.

Article 42A is the general interpretation provision for Part 3A. Article 42B confers the right to give a notice (an "Article 42B notice") requiring a person to use a key to render protected information in intelligible form and disclose the information or, if the person has the key but does not have and cannot get the protected information, to disclose the key. A notice can be given only in relation to protected information which has lawfully come into a person's possession, whether through the exercise of powers of entry, search and seizure or the exercise of powers under this Law or by any other means. Only a person having the appropriate permission, obtained in accordance with Schedule 2A, can give a notice. A notice can be given only in the interests of national security, to prevent or detect crime or in the interests of the economic well-being of Jersey. The requirement for disclosure must be proportionate to what is to be achieved and there must be no other reasonably practicable means by which the protected information can be rendered intelligible. The notice must restrict the persons to whom the key is disclosed.

Article 42C describes the effect of an Article 42B notice where the person to whom the notice is addressed has both the information and the key. It entitles that person to use the key and obtain the protected information in intelligible form. The person must then disclose the information or may instead disclose the key. If it transpires that the person does not have the information or cannot access it, the person is required instead to disclose any key to the information that he or she possesses.

Article 42D is concerned with Article 42B notices that can be complied with only by disclosure of a key. It requires the senior officer in the public authority by which the notice is given to issue or give permission for a direction specifying that the notice requires disclosure of the key. A direction can be given only if there are special circumstances that mean that, were the direction not given, the purposes of the requirement for disclosure would be defeated and that giving the direction is proportionate to what is to be achieved. The Investigatory Powers Commissioner must be notified within 7 days of a direction having been given by the Chief Officer of the States of Jersey Police or the Customs and Immigration Service.

Article 42E imposes a power for the States to enable a contribution to be made out of public funds to the costs incurred by persons complying with Article 42B notices.

Article 42F makes it an offence to fail to comply with an Article 42B notice for which the penalty is imprisonment for 5 years and/or an unlimited fine. If the person to whom the notice was given is shown to have been in possession of the key before the notice was given, there is a presumption that he or she continued to have possession of the key. However, the accused can rebut the presumption merely by adducing sufficient evidence to raise an issue with respect to his or her possession of the key. In that event, the prosecution must then prove beyond reasonable doubt that the accused had possession of the key after the notice was given.

Article 42G first enables a person giving an Article 42B notice to include in it a requirement to keep secret the contents of the notice and anything done pursuant to it and, secondly, makes it an offence to fail to comply with that requirement. A

requirement for secrecy can be included in the Article 42B notice only with the consent of the person who gave permission for the notice and only in order to maintain the effectiveness of the investigatory operations of the police, the Customs and Immigration Service or the intelligence services or in order to protect an individual. The penalty for the offence of failing to comply with a requirement to keep an Article 42B notice secret is imprisonment for up to 5 years and/or an unlimited fine. It is a defence if the disclosure took the form of the operation of software indicating that the key had ceased to be secure and the accused could not reasonably have been expected to take steps to prevent the disclosure. There is also a defence for disclosure protected by legal professional privilege and for disclosure to or authorized by the Investigatory Powers Commissioner or authorized by the person who gave the notice or the person in possession of the protected information. It is also a defence if the accused did not know or suspect that the notice contained a secrecy requirement.

Article 42H imposes duties on the Attorney General, any administration of the States or as Minister, the Chief Officer of the States of Jersey Police, the Agent of the Impôts, and every other person whose officers and employees include duties include giving Article 42B notices. The duties imposed are intended to ensure that keys are used only to obtain protected information, that there is minimum disclosure and copying of keys, that keys are stored in a secure manner and that records of disclosed keys are destroyed as soon as they are no longer needed. A person required to disclose a key or information or whose key or information is disclosed and who suffers any loss by reason of the breach of any duty imposed by this Article has a civil right of action.

Article 4(4)-(9) make amendments to the 2005 Law that are consequential on the insertion of Part 3A and *paragraph (10)* inserts Schedule 2A, which appears as a Schedule to the draft Law and provides for persons having the appropriate permission for the purposes of Part 3A.

Article 5 provides for the short title of the Law and for it to come into force 7 days after its registration.

DRAFT CYBERCRIME (JERSEY) LAW 201-

Arrangement

Article

Jersey

DRAFT CYBERCRIME (JERSEY) LAW 201-

A LAW to amend various Laws to give further effect to the Council of Europe Convention on Cybercrime (Budapest, 2001), to amend the Regulation of Investigatory Powers (Jersey) Law 2005[1] to provide for the investigation of electronic data protected by encryption and for connected purposes.

Adopted by the States	*[date to be inserted]*
Sanctioned by Order of Her Majesty in Council	*[date to be inserted]*
Registered by the Royal Court	*[date to be inserted]*

THE STATES, subject to the sanction of Her Most Excellent Majesty in Council, have adopted the following Law –

1 Amendment of Computer Misuse (Jersey) Law 1995

(1) The Computer Misuse (Jersey) Law 1995[2] is amended as follows.

(2) In Article 1 –

(a) paragraph (7) shall be deleted;

(b) for paragraph (8) there shall be substituted the following paragraph –

"(8) An act done in relation to a computer is unauthorized if the person doing the act (or causing it to be done) –

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

(b) does not have consent to the act from any such person,

and in this paragraph 'act' includes a series of acts.";

(c) after paragraph (9) there shall be inserted the following paragraph –

"(10) The States may by Regulations amend any definition in this Article.".

(3) In Article 2 –

(a) at the end of paragraph (1)(a) there shall be added the words ", or to enable any such access to be secured";

(b) in paragraph (1)(b) after the word "secure" there shall be inserted the words ", or to enable to be secured,";

(c) in paragraph (3) for the words from "not exceeding" to the end of the paragraph there shall be substituted the words "of 2 years and to a fine".

(4) For Article 5 there shall be substituted the following Articles –

"5 Unauthorized acts with intent to impair, or with recklessness as to impairing, operation of computer

(1) A person is guilty of an offence if –

(a) he or she does any unauthorized act in relation to a computer;

(b) at the time when the act is done he or she knows that it is unauthorized; and

(c) paragraph (2) applies.

(2) This paragraph applies if the person intends by doing the act to do any of the following, or is reckless as to whether the act will do any of the following –

(a) impair the operation of any computer;

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

(c) impair the operation of any such program or the reliability of any such data; or

(d) enable any of the things mentioned in sub-paragraphs (a) to (c) to be done.

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

(a) any particular computer;

(b) any particular program or data; or

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

(4) In this Article –

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

(b) 'act' includes a series of acts;

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

(5) A person guilty of an offence under this Article is liable to imprisonment for a term of 10 years and to a fine.

5A Making, supplying or obtaining articles for use in offence under Article 2 or 5

(1) A person is guilty of an offence if he or she 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 Article 2 or Article 5.

(2) A person is guilty of an offence if he or she 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 Article 2 or Article 5.

(3) A person is guilty of an offence if he or she obtains any article with a view to its being supplied for use to commit, or to assist in the commission of, an offence under Article 2 or Article 5.

(4) A person guilty of an offence under this Article is liable to imprisonment for a term of 2 years and to a fine.

(5) In this Article 'article' includes any program or data held in electronic form.".

2 Amendment of Criminal Justice (International Co-operation) (Jersey) Law 2001

After Article 5B of the Criminal Justice (International Co-operation) (Jersey) Law 2001[3] there shall be inserted the following Articles –

"5C Order to preserve data pending request for assistance

(1) Where an authority in a country or territory outside Jersey intends to submit a request for assistance under Article 5(1), that authority may request the Attorney General to apply to the court for an order (a 'preservation order') for the expeditious preservation of data stored by means of a computer system.

(2) The request to the Attorney General must specify –

(a) the authority seeking preservation;

(b) the offence that is the subject of a criminal investigation or proceedings together with a brief summary of the relevant facts;

(c) the data that is to be preserved and its relationship to the offence;

(d) any available information identifying the person in possession of the data or the computer system on which it is stored;

(e) the reason why the preservation is necessary; and

(f) that the authority intends to submit a request for assistance under Article 5(1) for assistance in obtaining the data.

(3) On receiving the application by or on behalf of the Attorney General under this Article the court may, where it considers it in the interests of justice to do so, make an order for the data to be preserved pending a request being made under Article 5(1) or for such time as the court thinks fit.

(4) An application for a preservation order may be made *ex parte* to the Bailiff in chambers.

(5) A preservation order must provide for notice to be given to any person named within it.

(6) A person named within a preservation order who by any act or omission causes the damage, deletion, alteration, suppression or removal of any data preserved by the order is guilty of an offence and liable to imprisonment for a term of 5 years and to a fine.

(7) A person named within a preservation order may apply to the Bailiff in chambers for the order to be revoked or varied and the Bailiff must either rule upon the application or refer it to the Royal Court.

5D Offence of unauthorized disclosure of preservation order

(1) Where an order is made under Article 5C(3) a person must not disclose –

(a) the existence and contents of the order;

(b) the details of the making of the order and of any variation of it;

(c) the existence and contents of any requirement to provide assistance with giving effect to the order;

(d) the steps taken in pursuance of the order or of any such requirement; and

(e) any part of the data preserved by the order.

(2) A person who contravenes paragraph (1) is guilty of an offence and liable to imprisonment for a term of 5 years and to a fine.

(3) In proceedings against any person for an offence under this Article in respect of any disclosure, it is a defence for the accused to show that the accused could not reasonably have been expected, after first becoming aware of any of the matters mentioned in paragraph (1), to take steps to prevent the disclosure.

(4) In proceedings against any person for an offence under this Article in respect of any disclosure, it is a defence for the accused to show that –

(a) the disclosure was made by or to a professional legal adviser in connection with the giving, by the adviser to any client of the adviser, of advice about the effect of any provision of this Law; and

(b) the person to whom or, as the case may be, by whom it was made was the client or a representative of the client.

(5) In proceedings against any person for an offence under this Article in respect of any disclosure, it is a defence for the accused to show that the disclosure was made by a professional legal adviser –

(a) in contemplation of, or in connection with, any legal proceedings; and

(b) for the purposes of those proceedings.

(6) Neither paragraph (4) nor paragraph (5) applies in the case of a disclosure made with a view to furthering any criminal purpose.".

3 Amendment of Police Procedures and Criminal Evidence (Jersey) Law 2003

(1) The Police Procedures and Criminal Evidence (Jersey) Law 2003[4] is amended as follows.

(2) For Article 16(1) there shall be substituted the following paragraphs –

"(1) A police officer may obtain access to material to which this Article applies for the purposes of a criminal investigation by making an application under Schedule 2 and in accordance with that Schedule.

(1A) This Article applies to –

(a) excluded material;

(b) special procedure material; and

(c) material stored on a computer or stored on a device that is remotely accessible via the internet and accessible by the person who stored it but not to users of the internet generally.".

(3) After Article 70 there shall be inserted the following Articles –

"70A Order to preserve data pending criminal investigation

(1) The court may make an order, referred to in this Law as a 'preservation order', on an application made by or on behalf of the Attorney General where it considers it is in the interests of justice to do so.

(2) A preservation order is an order providing that certain data specified in the application be preserved pending criminal investigation or for such time as the court thinks fit.

(3) An application for a preservation order may be made *ex parte* to the Bailiff in chambers.

(4) The court must not make a preservation order unless it is satisfied that there are reasonable grounds for believing –

(a) that a serious offence has been committed; and

(b) the data specified in the application includes evidence that relates to that offence or to some other offence that is connected with, or similar to, that offence.

(5) A preservation order must provide for notice to be given to any person named within it.

(6) A person named within a preservation order who by any act or omission causes the damage, deletion, alteration, suppression or removal of any data preserved by the order is guilty of an offence and liable to imprisonment for a term of 5 years and to a fine.

(7) A person named within a preservation order may apply to the Bailiff in chambers for the order to be revoked or varied and the Bailiff must rule upon the application or refer it to the Royal Court.

70B Offence of unauthorized disclosure of preservation order

(1) Where an order is made under Article 70A(1) a person must not disclose –

(a) the existence and contents of the order;

(b) the details of the making of the order and of any variation of it;

(c) the existence and contents of any requirement to provide assistance with giving effect to the order;

(d) the steps taken in pursuance of the order or of any such requirement; and

(e) any part of the data preserved by the order.

(2) A person who contravenes paragraph (1) is guilty of an offence and liable to imprisonment for a term of 5 years and to a fine.

(3) In proceedings against any person for an offence under this Article in respect of any disclosure, it is a defence for the accused to show that the accused could not reasonably have been expected, after first becoming aware of any of the matters mentioned in paragraph (1), to take steps to prevent the disclosure.

(4) In proceedings against any person for an offence under this Article in respect of any disclosure, it is a defence for the accused to show that –

(a) the disclosure was made by or to a professional legal adviser in connection with the giving, by the adviser to any client of the adviser, of advice about the effect of any provision of this Law; and

(b) the person to whom or, as the case may be, by whom it was made was the client or a representative of the client.

(5) In proceedings against any person for an offence under this Article in respect of any disclosure, it is a defence for the accused to show that the disclosure was made by a professional legal adviser –

(a) in contemplation of, or in connection with, any legal proceedings; and

(b) for the purposes of those proceedings.

(6) Neither paragraph (4) nor paragraph (5) applies in the case of a disclosure made with a view to furthering any criminal purpose.".

(4) In Schedule 2 –

(a) for the heading "SPECIAL PROCEDURE" there shall be substituted the heading "ACCESS TO CERTAIN MATERIAL";

(b) in paragraph 2(1)(a)(ii) for the words "which consists" to the end there shall be substituted the words "to which Article 16 applies

that is in the possession or control of a person, or on premises, specified in the application";

(c) in paragraph 3 after the word "possession" there shall be inserted the words "or control";

(d) in paragraph 11 for the words "enter and search the premises" there shall be substituted the words "search for the material and enter any premises necessary for the purposes of the search";

(e) in paragraph 13(a) for the words "the premises" there shall be substituted the words "any premises".

4 Amendment of Regulation of Investigatory Powers (Jersey) Law 2005

(1) The Regulation of Investigatory Powers (Jersey) Law 2005[5] is amended as follows.

(2) After Article 27 there shall be inserted the following Article –

"27A Offence of unauthorized disclosure by postal or telecommunications operator

(1) Where a notice is given to a postal or telecommunications operator under Article 26(4) it shall be the duty of that operator to keep secret the matters mentioned in paragraph (2).

(2) The matters to be kept secret are –

(a) the existence and contents of the notice given under Article 26(4);

(b) the details of the issue of the notice and of any renewal or modification of it;

(c) the existence and contents of any requirement to provide assistance with giving effect to the notice;

(d) the steps taken in pursuance of the notice or of any such requirement; and

(e) everything in the intercepted material, together with any related communications data.

(3) A person who makes a disclosure to another person of anything that he or she is required to keep secret under this Article is guilty of an offence and liable to imprisonment for a term of 5 years and to a fine.

(4) In proceedings against any person for an offence under this Article in respect of any disclosure, it is a defence for the accused to show that the accused could not reasonably have been expected, after being given the notice or (as the case may be) first becoming aware of the matter disclosed, to take steps to prevent the disclosure.

(5) In proceedings against any person for an offence under this Article in respect of any disclosure, it is a defence for the accused to show that –

(a) the disclosure was made by or to a professional legal adviser in connection with the giving, by the adviser to any client of the adviser, of advice about the effect of provisions of this Chapter; and

(b) the person to whom or, as the case may be, by whom it was made was the client or a representative of the client.

(6) In proceedings against any person for an offence under this Article in respect of any disclosure, it is a defence for the accused to show that the disclosure was made by a professional legal adviser –

(a) in contemplation of, or in connection with, any legal proceedings; and

(b) for the purposes of those proceedings.

(7) Neither paragraph (5) nor paragraph (6) applies in the case of a disclosure made with a view to furthering any criminal purpose.

(8) In proceedings against any person for an offence under this Article in respect of any disclosure, it is a defence for the accused to show that the disclosure was confined to a disclosure made to the Commissioner or authorized –

(a) by the Commissioner;

(b) by the terms of the notice;

(c) by or on behalf of the person who gave the notice; or

(d) by or on behalf of a person who –

(i) is in lawful possession of the protected information (within the meaning of Article 42A(1)) to which the notice relates, and

(ii) came into possession of that information.".

(3) After Part 3 there shall be inserted the following Part –

"PART 3A

INVESTIGATION OF ELECTRONIC DATA PROTECTED BY ENCRYPTION ETC.

42A Interpretation of Part 3A

(1) In this Part –

'electronic signature' means anything in electronic form that is –

(a) incorporated into, or otherwise logically associated with, any electronic communication or other electronic data;

(b) generated by the signatory or other source of the communication or data; and

(c) used for the purpose of facilitating, by means of a link between the signatory or other source and the communication or data, the establishment of the authenticity

of the communication or data, the establishment of its integrity, or both;

'key', in relation to any electronic data, means any key, code, password, algorithm, biometric identification or other data the use of which (with or without other keys) –

(a) allows access to the electronic data; or

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

'protected information' means any electronic data that, without the key to the data –

(a) cannot, or cannot readily, be accessed; or

(b) cannot, or cannot readily, be put into an intelligible form;

'Article 42B notice' means a notice under Article 42B;

'warrant' includes any authorization, notice or other instrument (however described) conferring a power of the same description as may, in other cases, be conferred by a warrant.

(2) References in this Part to a person's having information (including a key to protected information) in that person's possession include references –

(a) to its being in the possession of another person who is under that person's control so far as that information is concerned;

(b) to that person's having an immediate right of access to it, or an immediate right to have it transmitted or otherwise supplied to him or her; and

(c) to its being, or being contained in, anything which that person or another person under that person's control is entitled, in exercise of any statutory power and without otherwise taking possession of it, to detain, inspect or search.

(3) References in this Part to being in, or being put into, intelligible form include references to being in the condition in which the thing in question was before an encryption or similar process was applied to it or, as the case may be, to being restored to that condition.

(4) In this Article –

(a) references to the authenticity of any communication or data are references to any one or more of the following –

(i) whether the communication or data comes from a particular person or other source,

(ii) whether it is accurately timed and dated,

(iii) whether it is intended to have legal effect; and

(b) references to the integrity of any communication or data are references to whether there has been any tampering with or other modification of the communication or data.

42B Power to require disclosure of protected information or key

(1) This Article applies where any protected information –

(a) has come into the possession of any person by means of the exercise of a statutory power to seize, detain, inspect, search or otherwise to interfere with documents or other property, or is likely to do so;

(b) has come into the possession of any person by means of the exercise of any statutory power to intercept communications, or is likely to do so;

(c) has come into the possession of any person by means of the exercise of any power conferred by an authorization under Article 26(3) or under Part 3, or as a result of the giving of a notice under Article 26(4), or is likely to do so;

(d) has come into the possession of any person as a result of having been provided or disclosed in pursuance of any statutory duty (whether or not one arising as a result of a request for information), or is likely to do so; or

(e) has, by any other lawful means not involving the exercise of statutory powers, come into the possession of any of the intelligence services, the Force or the Agent of the Impôts or is likely so to come into the possession of any of them.

(2) If any person with the appropriate permission under Schedule 2A believes, on reasonable grounds –

(a) that a key to the protected information is in the possession of any person;

(b) that the imposition of a disclosure requirement in respect of the protected information is –

(i) necessary on grounds falling within paragraph (3), or

(ii) necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty;

(c) that the imposition of such a requirement is proportionate to what is sought to be achieved by its imposition; and

(d) that it is not reasonably practicable for the person with the appropriate permission to obtain possession of the protected information in an intelligible form without the giving of a notice under this Article,

the person with that permission may, by notice to the person whom he or she believes to have possession of the key, impose a disclosure requirement in respect of the protected information.

(3) A disclosure requirement in respect of any protected information is necessary on grounds falling within this paragraph if it is necessary –

(a) in the interests of national security;

(b) for the purpose of preventing or detecting crime; or

(c) in the interests of the economic well-being of Jersey.

(4) A notice under this Article imposing a disclosure requirement in respect of any protected information –

(a) must be given in writing or (if not in writing) must be given in a manner that produces a record of its having been given;

(b) must describe the protected information to which the notice relates;

(c) must specify the matters falling within paragraph (2)(b)(i) or (ii) by reference to which the notice is given;

(d) must specify the office, rank or position held by the person giving it;

(e) must specify the office, rank or position of the person who, for the purposes of Schedule 2A, granted permission for the giving of the notice or (if the person giving the notice was entitled to give it without another person's permission) must set out the circumstances in which that entitlement arose;

(f) must specify the time by which the notice is to be complied with; and

(g) must set out the disclosure that is required by the notice and the form and manner in which it is to be made,

and the time specified for the purposes of sub-paragraph (f) must allow a period for compliance which is reasonable in all the circumstances.

(5) Where it appears to a person with the appropriate permission –

(a) that more than one person is in possession of the key to any protected information;

(b) that any of those persons is in possession of that key in that person's capacity as an officer or employee of any body corporate; and

(c) that another of those persons is the body corporate itself or another officer or employee of the body corporate,

a notice under this Article may not be given, by reference to a person's possession of the key, to any officer or employee of the body corporate unless that person is a senior officer of the body corporate or it appears to the person giving the notice that there is no senior officer of the body corporate and (in the case of an employee) no more senior employee of the body corporate to whom it is reasonably practicable to give the notice.

(6) Where it appears to a person with the appropriate permission –

(a) that more than one person is in possession of the key to any protected information;

(b) that any of those persons is in possession of that key in that person's capacity as an employee of a firm; and

(c) that another of those persons is the firm itself or a partner of the firm,

a notice under this Article may not be given, by reference to a person's possession of the key, to any employee of the firm unless it appears to the person giving the notice that there is neither a partner of the firm nor a more senior employee of the firm to whom it is reasonably practicable to give the notice.

(7) Paragraphs (5) and (6) do not apply to the extent that there are special circumstances of the case that mean that the purposes for which the notice is given would be defeated, in whole or in part, if the notice were given to the person to whom it would otherwise be required to be given by those paragraphs.

(8) A notice under this Article may not require the making of any disclosure to any person other than –

(a) the person giving the notice; or

(b) such other person as may be specified in or otherwise identified by, or in accordance with, the provisions of the notice.

(9) A notice under this Article may not require the disclosure of any key that –

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

(b) has not in fact been used for any other purpose.

(10) In this Article 'senior officer', in relation to a body corporate, means a director, manager, secretary or other similar officer of the body corporate; and for this purpose 'director', in relation to a body corporate whose affairs are managed by its members, means a member of the body corporate.

42C Effect of notice imposing disclosure requirement

(1) Subject to the following provisions of this Article, the effect of an Article 42B notice imposing a disclosure requirement in respect of any protected information on a person who is in possession at a relevant time of both the protected information and a means of obtaining access to the information and of disclosing it in an intelligible form is that the person –

(a) is entitled to use any key in his or her possession to obtain access to the information or to put it into an intelligible form; and

(b) is required, in accordance with that notice, to make a disclosure of the information in an intelligible form.

(2) A person subject to a requirement to make disclosure under paragraph (1)(b) is taken to have complied with that requirement if –

(a) the person makes instead a disclosure of any key to the protected information that is in his or her possession; and

(b) that disclosure is made, in accordance with the notice imposing the requirement, to the person to whom, and by the

time by which, he or she was required to provide the information in that form.

(3) Where a disclosure requirement in respect of any protected information is imposed on any person by an Article 42B notice and –

(a) that person is not in possession of the information;

(b) that person is incapable, without the use of a key that is not in his or her possession, of obtaining access to the information and of disclosing it in an intelligible form; or

(c) the notice states, in pursuance of a direction under Article 42D, that it can be complied with only by the disclosure of a key to the information,

the effect of imposing that disclosure requirement on that person is to require the person, in accordance with the notice imposing the requirement, to make a disclosure of any key to the protected information that is in his or her possession at a relevant time.

(4) Paragraphs (5) to (7) apply where a person ('the person given notice') –

(a) is entitled or obliged to disclose a key to protected information for the purpose of complying with any disclosure requirement imposed by an Article 42B notice; and

(b) is in possession of more than one key to that information.

(5) It is not necessary, for the purpose of complying with the requirement, for the person given notice to make a disclosure of any keys in addition to those the disclosure of which is, alone, sufficient to enable the person to whom they are disclosed to obtain access to the information and to put it into an intelligible form.

(6) Where –

(a) paragraph (5) allows the person given notice to comply with a requirement without disclosing all of the keys in that person's possession; and

(b) there are different keys, or combinations of keys, in the possession of that person the disclosure of which would, under that paragraph, constitute compliance,

the person given notice may select which of the keys, or combination of keys, to disclose for the purpose of complying with that requirement in accordance with that paragraph.

(7) Subject to paragraphs (5) and (6), the person given notice is not to be taken to have complied with the disclosure requirement by the disclosure of a key unless that person has disclosed every key to the protected information that is in his or her possession at a relevant time.

(8) Where, in a case in which a disclosure requirement in respect of any protected information is imposed on any person by an Article 42B notice –

(a) that person has been in possession of the key to that information but is no longer in possession of it;

(b) if that person had continued to be in possession of the key, he or she would have been required by virtue of the giving of the notice to disclose it; and

(c) that person is in possession, at a relevant time, of information to which paragraph (9) applies,

the effect of imposing the disclosure requirement on that person is to require that person, in accordance with the notice, to disclose all such information to which paragraph (9) applies as is in that person's possession and as that person may be required, in accordance with the notice, to disclose by the person to whom he or she would have been required to disclose the key.

(9) This paragraph applies to any information that would facilitate the obtaining or discovery of the key or the putting of the protected information into an intelligible form.

(10) In this Article 'relevant time', in relation to a disclosure requirement imposed by an Article 42B notice, means the time of the giving of the notice or any subsequent time before the time by which the requirement falls to be complied with.

42D Cases in which key required

(1) An Article 42B notice must not contain a statement for the purposes of Article 42C(3)(c) unless –

(a) the person who, for the purposes of Schedule 2A, granted the permission for the giving of the notice; or

(b) any person whose permission for the giving of such a notice in relation to that information would constitute the appropriate permission for the purposes of that Schedule,

has given a direction that the requirement can be complied with only by the disclosure of the key itself.

(2) A direction for the purposes of paragraph (1) by the Force or the States of Jersey Customs and Immigration Service must be given only by or with the permission of the Chief Officer or the Agent of the Impôts, as the case may be, expressly in relation to the direction in question.

(3) A person must not give a direction for the purposes of paragraph (1) unless the person believes –

(a) that there are special circumstances that mean that the purposes for which it was believed necessary to impose the requirement in question would be defeated, in whole or in part, if the direction were not given; and

(b) that the giving of the direction is proportionate to what is sought to be achieved by prohibiting any compliance with the requirement in question otherwise than by the disclosure of the key itself.

(4) The matters to be taken into account in considering whether the requirement of paragraph (3)(b) is satisfied in the case of any direction include –

(a) the extent and nature of any protected information, in addition to the protected information in respect of which the disclosure requirement is imposed, to which the key is also a key; and

(b) any adverse effect that the giving of the direction might have on a business carried on by the person on whom the disclosure requirement is imposed.

(5) Where a direction for the purposes of paragraph (1) is given by or with the permission of the Chief Officer or the Agent of the Impôts, the person giving the direction must notify the Commissioner that the direction has been given.

(6) A notification under paragraph (5) –

(a) must be given no later than 7 days after the day of the giving of the direction to which it relates; and

(b) may be given either in writing or by being transmitted to the Commissioner by electronic means.

42E Contribution to costs of disclosure

(1) The States may ensure that such arrangements as they think appropriate are in place to require or authorize, in such cases as they think fit, the making of appropriate contributions towards the costs incurred by persons to whom Article 42B notices are given in complying with such notices.

(2) Contributions made under this Article must be paid out of the annual income of the States.

42F Offence: failure to comply with a notice

(1) It is an offence for a person to whom an Article 42B notice has been given knowingly to fail to make the disclosure required by the giving of the notice and in accordance with the notice.

(2) In proceedings against any person for an offence under this Article, if it is shown that the accused was in possession of a key to any protected information at any time before the time of the giving of the Article 42B notice, the accused is taken for the purposes of those proceedings to have continued to be in possession of that key at all subsequent times, unless it is shown that the key was not in the accused's possession after the giving of the notice and before the time by which the accused was required to disclose it.

(3) For the purposes of this Article a person is taken to have shown that he or she was not in possession of a key to protected information at a particular time if –

(a) sufficient evidence of that fact is adduced to raise an issue with respect to it; and

(b) the contrary is not proved beyond a reasonable doubt.

(4) In proceedings against any person for an offence under this Article it shall be a defence for the accused to show –

(a) that it was not reasonably practicable for the accused to make the disclosure required by virtue of the giving of the Article 42B notice by the time by which the accused was required, in accordance with that notice, to make it; but

(b) that the accused did make that disclosure as soon after that time as it was reasonably practicable for the accused to do so.

(5) A person guilty of an offence under this Article is liable to imprisonment for a term of 5 years and to a fine.

42G Offence: tipping-off

(1) This Article applies where an Article 42B notice contains a provision requiring –

(a) the person to whom the notice is given; and

(b) every other person who becomes aware of it or of its contents,

to keep secret the giving of the notice, its contents and the things done in pursuance of it.

(2) A requirement to keep anything secret must not be included in an Article 42B notice except where –

(a) it is included with the consent of the person who, for the purposes of Schedule 2A, granted the permission for the giving of the notice; or

(b) the person who gives the notice is also a person whose permission for the giving of such a notice in relation to the information in question would constitute appropriate permission for the purposes of that Schedule.

(3) An Article 42B notice must not contain a requirement to keep anything secret except where the protected information to which it relates –

(a) has come into the possession of the Force, the States of Jersey Customs and Immigration Service or any of the intelligence services; or

(b) is likely to come into the possession of any of the bodies mentioned in sub-paragraph (a),

by means which it is reasonable, in order to maintain the effectiveness of any investigation or operation or of investigatory techniques generally, or in the interests of the safety or well-being of any person, to keep secret from a particular person.

(4) A person who makes a disclosure to any other person of anything that he or she is required by an Article 42B notice to keep secret is guilty of an offence and liable to imprisonment for a term of 5 years and to a fine.

(5) In proceedings against any person for an offence under this Article in respect of any disclosure, it is a defence for the accused to show that –

(a) the disclosure was effected entirely by the operation of software designed to indicate when a key to protected information has ceased to be secure; and

(b) the accused could not reasonably have been expected to take steps, after being given the notice or (as the case may be) becoming aware of it or of its contents, to prevent the disclosure.

(6) In proceedings against any person for an offence under this Article in respect of any disclosure, it is a defence for the accused to show that –

(a) the disclosure was made by or to a professional legal adviser in connection with the giving, by the adviser to any client of the adviser's, of advice about the effect of provisions of this Part; and

(b) the person to whom or, as the case may be, by whom it was made was the client or a representative of the client.

(7) In proceedings against any person for an offence under this Article in respect of any disclosure, it is a defence for the accused to show that the disclosure was made by a professional legal adviser –

(a) in contemplation of, or in connection with, any legal proceedings; and

(b) for the purposes of those proceedings.

(8) Neither paragraph (6) nor paragraph (7) applies in the case of a disclosure made with a view to furthering any criminal purpose.

(9) In proceedings against any person for an offence under this Article in respect of any disclosure, it is a defence for the accused to show that the disclosure was confined to a disclosure made to the Commissioner or authorized –

(a) by the Commissioner;

(b) by the terms of the notice;

(c) by or on behalf of the person who gave the notice; or

(d) by or on behalf of a person who –

(i) is in lawful possession of the protected information to which the notice relates, and

(ii) came into possession of that information as mentioned in Article 42B(1).

(10) In proceedings for an offence under this Article against a person other than the person to whom the notice was given, it is a defence

for the accused to show that the accused neither knew nor had reasonable grounds for suspecting that the notice contained a requirement to keep secret what was disclosed.

42H General duties of specified authorities

(1) This Article applies to –

(a) the Attorney General;

(b) any administration of the States or a Minister;

(c) the Chief Officer of the Force or the Agent of the Impôts;

(d) every other person whose officers or employees include persons with duties that involve the giving of Article 42B notices.

(2) Each of the persons to whom this Article applies must ensure that such arrangements are in place, in relation to persons under his or her control who by virtue of this Part obtain possession of keys to protected information, as that person considers necessary for securing –

(a) that a key disclosed in pursuance of an Article 42B notice is used for obtaining access to, or putting into an intelligible form, only protected information in relation to which the power to give such a notice was exercised or could have been exercised if the key had not already been disclosed;

(b) that the uses to which a key so disclosed is put are reasonable having regard both to the uses to which the person using the key is entitled to put any protected information to which it relates and to the other circumstances of the case;

(c) that, having regard to those matters, the use and any retention of the key are proportionate to what is sought to be achieved by its use or retention;

(d) that the requirements of paragraph (3) are satisfied in relation to any key disclosed in pursuance of an Article 42B notice;

(e) that, for the purpose of ensuring that those requirements are satisfied, any key so disclosed is stored, for so long as it is retained, in a secure manner;

(f) that all records of a key so disclosed (if not destroyed earlier) are destroyed as soon as the key is no longer needed for the purpose of enabling protected information to be put into an intelligible form.

(3) The requirements of this paragraph are satisfied in relation to any key disclosed in pursuance of an Article 42B notice if –

(a) the number of persons to whom the key is disclosed or otherwise made available; and

(b) the number of copies made of the key,

are each limited to the minimum that is necessary for the purpose of enabling protected information to be put into an intelligible form.

(4) Subject to paragraph (5), where any relevant person incurs any loss or damage in consequence of –

(a) any breach by a person to whom this Article applies of the duty imposed on that person by paragraph (2); or

(b) any contravention by any person whatever of arrangements made under that paragraph in relation to persons under the control of a person to whom this Article applies,

the breach or contravention is actionable against the person to whom this Article applies at the suit or instance of the relevant person.

(5) A person is a relevant person for the purposes of paragraph (4) if that person –

(a) has made a disclosure in pursuance of an Article 42B notice; or

(b) is a person whose protected information or key has been disclosed in pursuance of such a notice,

and loss or damage shall be taken into account for the purposes of that paragraph to the extent only that it relates to the disclosure of particular protected information or a particular key which, in the case of a person falling within sub-paragraph (b), must be that person's information or key.

(6) For the purposes of paragraph (5) –

(a) information belongs to a person if that person has any right that would be infringed by an unauthorized disclosure of the information; and

(b) a key belongs to a person –

(i) if it is a key to information that belongs to that person, or

(ii) if that person has any right that would be infringed by an unauthorized disclosure of the key.

(7) In any proceedings brought by virtue of paragraph (4), the court must have regard to any opinion with respect to the matters to which the proceedings relate that is or has been given by the Commissioner.".

(4) In Article 43(2) after sub-paragraph (d) there shall be added the following sub-paragraphs –

"(e) the exercise and performance, by any person other than the Bailiff, of the powers and duties conferred or imposed, otherwise than with the permission of the Bailiff, by or under Part 3A;

(f) the adequacy of the arrangements by virtue of which the duties imposed by Article 42H are sought to be discharged

in relation to persons whose conduct is under review under sub-paragraph (b).".

(5) In Article 44 –

(a) in paragraph (1), the word "and" following sub-paragraph (m) shall be deleted and after sub-paragraph (m) there shall be inserted the following sub-paragraph –

"(ma) every person to whom a notice under Article 42B has been given in relation to any information obtained under Part 2; and";

(b) in paragraph (1)(n) for the words "(j) or (l)" there shall be substituted the words "(j), (l) or (ma)";

(c) in paragraph (3) for the words "duty imposed by Article 19 has" there shall be substituted the words "duties imposed by Articles 19 and 42H have".

(6) In Article 46 –

(a) in paragraph (4) the word "or" following sub-paragraph (b) shall be deleted and after sub-paragraph (b) there shall be inserted the following sub-paragraph –

"(ba) they are proceedings brought by virtue of Article 42H(4); or";

(b) in paragraph (6) after sub-paragraph (e) there shall be added the following sub-paragraph –

"(f) the giving of a notice under Article 42B or any disclosure or use of a key to protected information.";

(c) in paragraph (9) after sub-paragraph (c) there shall be inserted the following sub-paragraphs –

"(ca) a permission for the purposes of Schedule 2A;

(cb) a notice under Article 42B;";

(d) after paragraph (10) there shall be added the following paragraph –

"(11) In this Article –

(a) references to a key and to protected information shall be construed in accordance with Article 42A(1);

(b) references to the disclosure or use of a key to protected information taking place in relation to a person are references to such a disclosure or use taking place in a case in which that person has had possession of the key or of the protected information; and

(c) references to the disclosure of a key to protected information include references to the making of any disclosure in an intelligible form (within the meaning of Article 42A(3)) of protected information by a person who is or has been in possession of the key to that information,

and the reference in sub-paragraph (b) to a person's having possession of a key or of protected information shall be construed in accordance with Article 42A(2).".

(7) In Article 49(7) –

(a) after sub-paragraph (o) the word "and" shall be deleted and there shall be inserted the following sub-paragraph –

"(oa) every person to whom a notice under Article 42B has been given; and";

(b) in sub-paragraph (p) for the words "paragraph (h), (i) or (k)" there shall be substituted the words "sub-paragraph (h), (i), (k) or (oa)".

(8) In Article 51(2)(a) for the words "Parts 2 and 3" there shall be substituted the words "Parts 2, 3 and 3A".

(9) In Article 56(1) after the words "under this Law" there shall be inserted the words ", other than an offence under any provision of Part 3A,".

(10) After Schedule 2 there shall be inserted the Schedule set out in the Schedule to this Law.

5 Citation and commencement

This Law may be cited as the Cybercrime (Jersey) Law 201- and shall come into force 7 days after its registration.

SCHEDULE

(Article 4(10))

SCHEDULE 2A INSERTED

"SCHEDULE 2A

(Articles 42B(2), 42D(1)(a), 42G(2)(a), 46(9)(ca))

PERSONS HAVING THE APPROPRIATE PERMISSION

1 Interpretation

In this Schedule –

(a) 'authorization to interfere with property' means an authorization given under Article 101 of the Police Procedures and Criminal Evidence (Jersey) Law 2003[6];

(b) words and phrases defined in Part 3A shall have the same respective meanings.

2 General rule for appropriate permission

(1) Subject to the following provisions of this Schedule, a person has the appropriate permission in relation to any protected information if, and only if, written permission for the giving of Article 42B notices in relation to that information has been granted by the Bailiff or a Jurat.

(2) Nothing in paragraphs 3 and 4 providing for the manner in which a person may be granted the appropriate permission in relation to any protected information without a grant under this paragraph shall be construed as requiring any further permission to be obtained in a case in which permission has been granted under this paragraph.

3 Data obtained under warrant or under authorization of Attorney General

(1) This paragraph applies in the case of protected information falling within Article 42B(1)(a), (b) or (c) where the statutory power in question is one exercised, or to be exercised, in accordance with –

(a) a warrant issued by the Bailiff or a Jurat; or

(b) an interception warrant or authorization to interfere with property issued by the Attorney General.

(2) Subject to sub-paragraphs (3) to (5) and paragraph 5(1), a person has the appropriate permission in relation to that protected information (without any grant of permission under paragraph 2) if –

(a) the warrant or, as the case may be, the authorization contained the relevant authority's permission for the giving

of Article 42B notices in relation to protected information to be obtained under the warrant or authorization; or

(b) since the issue of the warrant or authorization, written permission has been granted by the relevant authority for the giving of such notices in relation to protected information obtained under the warrant or authorization.

(3) Only a person who –

(a) was entitled to exercise the power conferred by the warrant; or

(b) is of the description of persons on whom the power conferred by the warrant was, or could have been, conferred,

is capable of having the appropriate permission in relation to protected information obtained, or to be obtained, under a warrant issued by the Bailiff or a Jurat.

(4) Only persons holding office in any administration of the States or who are employed by the States' Employment Board established by Article 4(1) of the Employment of States of Jersey Employees (Jersey) Law 2005[7], or police officers in the Force are capable of having the appropriate permission in relation to protected information obtained, or to be obtained, under a warrant issued by the Attorney General.

(5) Only the Force and the States of Jersey Customs and Immigration Service are capable of having the appropriate permission in relation to protected information obtained, or to be obtained, under an authorization to interfere with property issued by the Attorney General.

(6) In this paragraph 'relevant authority' –

(a) in relation to a warrant issued by the Bailiff or a Jurat, means any person holding any judicial office that would have entitled that person to issue the warrant; and

(b) in relation to any warrant or an authorization to interfere with property issued by the Attorney General, means the Attorney General.

(7) Protected information that comes into a person's possession by means of the exercise of any statutory power which –

(a) is exercisable without a warrant; but

(b) is so exercisable in the course of, or in connection with, the exercise of another statutory power for which a warrant is required,

is not to be taken, by reason only of the warrant required for the exercise of the power mentioned in clause (b), to be information in the case of which this paragraph applies.

4 Data obtained under any enactment without a warrant or an authorization issued by the Attorney General

(1) This paragraph applies –

(a) in the case of protected information falling within Article 42B(1)(a), (b) or (c) that is not information in the case of which paragraph 3 applies; and

(b) in the case of protected information falling within Article 42B(1)(d) that is not information also falling within Article 42B(1)(a), (b) or (c).

(2) Subject to paragraph 5, where –

(a) the power conferred by the enactment was exercised, or is likely to be exercised, by the Force or the States of Jersey Customs and Immigration Service; or

(b) the information was provided or disclosed, or is likely to be provided or disclosed, to either of those bodies; or

(c) the information is in the possession of, or is likely to come into the possession of, either of those bodies,

the bodies have the appropriate permission in relation to the protected information, without any grant of permission under paragraph 2.

(3) In any other case a person does not have the appropriate permission by virtue of a grant of permission under paragraph 2 unless that person is a person falling within sub-paragraph (4).

(4) A person falls within this sub-paragraph if, as the case may be –

(a) he or she is the person who exercised the power conferred by an enactment or is of the description of persons who would have been entitled to exercise it;

(b) he or she is the person to whom the protected information was provided or disclosed, or is of a description of person the provision or disclosure of the information to whom would have discharged the statutory duty; or

(c) he or she is a person who is likely to be a person falling within clause (a) or (b) when the power is exercised or the protected information provided or disclosed.

5 General requirements relating to the appropriate permission

(1) A person does not have the appropriate permission in relation to any protected information unless the person is either –

(a) a person who has the protected information in his or her possession or is likely to obtain possession of it; or

(b) a person who is authorized (apart from this Law) to act on behalf of such a person.

(2) Subject to sub-paragraph (3), an officer of the Force does not by virtue of paragraph 3 or 4 have the appropriate permission in relation to any protected information unless –

(a) he or she is of or above the rank of inspector; or

(b) permission to give an Article 42B notice in relation to that information has been granted by a person holding the rank of inspector, or any higher rank.

(3) In the case of protected information that has come into the possession of the Force by means of the exercise of powers conferred by Article 40 of the Terrorism (Jersey) Law 2002[8], the permission required by sub-paragraph (2) shall not be granted by any person below the rank mentioned in paragraph (4) of that Article.

6 Duration of permission

(1) A permission granted by any person under any provision of this Schedule does not entitle any person to give an Article 42B notice at any time after the permission has ceased to have effect.

(2) Such a permission, once granted, continues to have effect (despite the cancellation, expiry or other discharge of any warrant or authorization in which it is contained or to which it relates) until such time (if any) as it –

(a) expires in accordance with any limitation on its duration that was contained in its terms; or

(b) is withdrawn by the person who granted it or by a person holding any office or other position that would have entitled that person to grant it.

7 Formalities for permissions granted by the Attorney General

Where any provision of this Schedule requires a warrant or an authorization to be issued by the Attorney General, the Attorney General may authorize any other person to issue the warrant or authorization on his or her behalf.".

[1] *chapter 08.830*
[2] *chapter 08.080*
[3] *chapter 08.300*
[4] *chapter 23.750*
[5] *chapter 08.830*
[6] *chapter 23.750*
[7] *chapter 16.325*
[8] *chapter 17.860*