STATES OF JERSEY

r

DRAFT REGULATION OF INVESTIGATORY POWERS (JERSEY) LAW 200-

Lodged au Greffe on 24th June 2003
by the Home Affairs Committee

STATES GREFFE

DRAFT REGULATION OF INVESTIGATORY POWERS (JERSEY) LAW 200-

European Convention on Human Rights

The President of the Home Affairs Committee has made the following statement –

In the view of the Home Affairs Committee the provisions of the Draft Regulation of Investigatory Powers (Jersey) Law 200- are compatible with the Convention Rights.

(Signed) **Senator W. Kinnard**

REPORT

A consequence of the enactment of the Human Rights (Jersey) Law 2000 is that a considerable number of new legislative provisions are needed in the areas of police practices and procedures and the gathering of evidence and intelligence, to make the law in Jersey compatible with the Convention rights.

Of the major areas of concern, in this regard, those relating to detention and questioning of suspects by the police, powers of entry, issue and execution of search warrants and the use of intrusive surveillance methods affecting property, are covered by the Police Procedures and Criminal Evidence (Jersey) Law ("PPCE").

The other areas, interception of communications and the use of covert and directed surveillance, will be covered by this draft Law, the Regulation of Investigatory Powers (Jersey) Law 200-.

It would be unwise, if not impracticable, to bring the Human Rights Law into effect without having the measures comprising the draft Law in place first. Without them, much of the work of the police (and other agencies) in gathering intelligence and evidence by interception of communications and from covert sources could be open to challenge on the commencement of the Human Rights Law and the police operations against crime and indeed the criminal justice system could be very seriously prejudiced.

Also, since the decision of the European Court of Human Rights in Halford -v- United Kingdom (1997), the case concerning the senior Manchester woman police officer whose phone calls carried on the Manchester Police internal telephone system were intercepted in the course of an internal investigation, it has been clear that interception of private, as well as public telecommunications, without statutory regulation is in breach of the individual's Convention rights.

The need for change in these areas of the law is not, however, wholly driven by human rights considerations. Rapid developments in communications technology in the past ten years or so, have made it necessary to make substantial modifications in the current Law relating to interception of communications for law enforcement purposes, the Interception of Communications (Jersey) Law 1993.

But the main driver is the development of the jurisprudence of the European Court of Human Rights and the establishment, by the Human Rights Law, of new means for enforcing, in the Courts in Jersey, compliance with the Convention rights.

When the Human Rights Law comes into force, all the laws in Jersey, whether statutory or customary will have to be given effect, as far as possible, in a way which is compatible with the Convention rights and all public authorities, including the police and other law enforcement agencies, will be under a duty to act compatibly with the Convention rights. Evidence gathered by intrusive or covert means will be routinely challenged in the courts if it has not been obtained under a statutory regime, compatible with the Convention rights, in particular, the right to respect for private and family life, home and correspondence guaranteed by Article 8 of the Convention.

Modern communications technology helps criminals, as well as those fighting crime, and it is essential that law enforcement is not hampered by the lack of a proper legal basis for making the most of the opportunities offered by such technology to prevent crime and track down offenders. Covert and intrusive methods of surveillance, whether mechanical or by persons and the use of informants is important, and will become, ever more important.

Such investigative methods, which are inevitably intrusive and by their very nature, take place out of the sight and cognisance of the subject of them and indeed others who may be accidentally affected by them, must be controlled and monitored under a statutory system which, while it does not interfere with or reduce the effectiveness of law enforcement, is and can be seen by the public to be, sufficient to provide confidence that it is operated properly, with a degree of independent scrutiny.

This is not to suggest that the law enforcement agencies currently act improperly or abuse their position, but rather that the advent of effective and enforceable remedies for breach of human rights, requires that the present system is put on a proper legal base.

As mentioned, in Convention terms, the main area for concern is the Article 8 right to respect for private and family life, home and correspondence. Interference with that right by a public authority must be proportionate and must have a basis in law which is identifiable and established, accessible (i.e. written down and available to be read), and clear, so that the consequences of a breach of the law can be foreseen.

If the present arrangements in Jersey for authorising covert or intrusive surveillance were found not to meet these

requirements, the grounds for lawful interference with the Article 8 right, such as for the prevention of crime or disorder, national security or the protection of health and morals, could not be utilised.

A recent illustration of the problem that could be faced in Jersey is to be found in the decision of the European Court of Human Rights in the case of Armstrong -v-United Kingdom, (16th July 2002), where the Court held, following its earlier decision in the case of Khan -v- United Kingdom (2000) that evidence obtained by means of a tape recorder secretly placed by the police in a flat belonging to one of the defendant's co-accused, had been obtained in breach of Article 8 because at the time when it was obtained, during 1994 and 1995, there was no statutory system to regulate the use of covert recording devices by the police. The interference with the defendant's private life was therefore not in accordance with the law, as required by Article 8.2 of the Convention.

An outline description of scheme of the draft Law is given below. Further detail about the individual provisions is contained in the accompanying Explanatory Note.

AN OUTLINE REVIEW OF THE DRAFT LAW

Part 1 – Introductory contains interpretation provisions, defining various important terms used in the draft Law.

Part 2, Chapter I – Interception of communications

This will make new provision in place of the Interception of Communications (Jersey) Law, 1993, which will be repealed. It will go further than the 1993 Law because this Part is concerned with interception of communications transmitted by public postal service or public telecommunication system and, for the first time, in Jersey, private telecommunications systems as well.

Interception by a public authority will require either lawful authority or an interceptions warrant. Otherwise, intercepting a public postal or telecommunications as well as interception of private telecommunications will be an offence. Provisions in this Part describe circumstances where there is lawful authority.

This Part also creates a new civil right for an individual to sue, in some circumstances, where his or her messages carried on a private telecommunications network are intercepted.

The Attorney General will be empowered to issue interception warrants. Only the Chief Police Officer, the Agent of the Impôts, the Chief Inspector of Immigration, the head of one of the intelligence services, the Chief of Defence Intelligence in the Ministry of defence or the competent authority of a country or territory outside the Island may apply for a warrant.

The interception warrant will have to relate either to a named person, as the subject, or a single set of premises, and must contain details of the apparatus, address, phone numbers relied on to identify the communications to be intercepted. These details will not need to be given if the communications are sent or received outside Jersey and the Attorney General has given a certificate in relation to the warrant.

An interception warrant will be implemented by the person to whom it is addressed, but that person may require others to assist, such as a person providing a postal or telecommunications service.

The Attorney General will have to ensure that there are restrictions on the persons to whom information obtained under an interceptions warrant may be disclosed.

The Committee will be able to require providers of postal or telecommunications services to maintain arrangements or facilities to make it possible to comply with interception warrants. If the Committee does so, the States will have to make arrangements for providers to receive contributions to the costs incurred.

Part 2, Chapter II – Acquisition and disclosure of communications data

This will provide for the circumstances under which law enforcement and other agencies can require disclosure of communications data or may serve notice on a telecommunications or postal operators to obtain or disclose communications data. This is not the contents of the communications but, rather, information about the sending apparatus, and the number, times, origins and destinations of communications (e.g. a log of phone calls).

Designated persons are listed in the Law and may be added to by the States by Regulations.

A designated person will be able to –

(a) give an authorisation to persons within his or her own organisation (or, in the Attorney General's case, persons within the applying public body or intelligence service) to engage in conduct to which Chapter 2 applies (conduct for obtaining communications data, but not the interception of communications, as that is catered for by Chapter 1) and the disclosure of communications data; and

(b) give notice requiring a postal or telecommunications operator to obtain and disclose communications data.

The States will need to make appropriate arrangements for providers to receive contributions to the costs incurred in complying with disclosure notices in such cases as they think fit.

Part 3 – Surveillance and Covert Human Intelligence sources

This Part would place on a statutory basis the use and authorisation of directed surveillance, intrusive surveillance and the conduct and use of covert human intelligence sources. Note that surveillance that involves entry into, or interference with, property or wireless telegraphy will be covered by the PPCE Law. The sort of conduct that would be covered by this Part will include the use of people to keep suspects under observation and the use of informants. Directed surveillance is covert (but not intrusive) surveillance for a specific investigation or operation and which is likely to result in obtaining private information about a person.

Intrusive surveillance is covert surveillance of anything happening in residential premises or in a private vehicle,

which term includes a vessel or aircraft, either by means of an individual on the premises or in the vehicle or by means of a surveillance device. The device must be actually on the premises or vehicle, unless it is capable of providing the same information as might be obtained from a device actually on the premises or vehicle. Intrusive surveillance does not include the use of a vehicle tracking device or the interception of communications. Covert human intelligence source is the use of a specialist officer handling informants, or an informant to obtain information by means of a relationship with a person without that person being aware of the purpose for which the information is obtained or the use to which it will be put.

Part 4 – Electronic data protected by encryption

This Part would create new powers for law enforcement agencies to demand that encrypted material, which has already been lawfully obtained, be rendered intelligible or that the key to its decryption be handed over. There will be a number of very specific requirements for obtaining the necessary orders and to protect the interests of the persons to whom the key belongs, including rights to take action if the duty to safeguard the key is breached and damage results to the person who made the disclosure or to the person to whom the key belonged. Information might lawfully come into a person's possession through the exercise of powers under this Law or under other Laws (i.e. any search warrant) or where information is provided in discharge of a statutory duty, or where information is simply passed to the person.

Protected information is electronic data which cannot be readily accessed or put into intelligible form - it needs either a password or decryption (the key).

A person given permission will be able to give notice –

- to another person who has the key and access to the information to use the key to render the information in intelligible form and disclose that information, or
- if the person has the key but does not have and cannot get the information, to disclose the key to the protected information.

The Bailiff or a Jurat will be able to give permission for the giving of an notice in every case. The Attorney General will also be able to do so where he has given an interception or other warrant. The police and Customs and Excise will be treated as having been given permission where their own "designated person" has given an authorisation under Part 2, Chapter 2.

The States will have to make arrangements for contributions to be made to the costs incurred by persons complying with Article 41 notices (Article 44).

A notice will include a requirement to keep the notice secret (Article 46). Disclosing the secret will be an offence.

The Attorney General and chief officers of organisations likely to require the disclosure of keys will be under a duty for the safekeeping and protection of keys.

Part 5 – Scrutiny of investigatory powers

This Part would make provision for the appointment of a Commissioner, who will be a judge of the Court of Appeal, who will oversee the exercise of the powers contained in the Law. A Tribunal will be established which will consider complaints about the exercise of the powers. The Commissioner will keep under review the exercise of all investigatory powers. He will report any unsatisfactory exercises of powers to the Bailiff. He will also prepare an annual report and submit it to the Bailiff. The Bailiff will arrange for it to be laid before the States.

The Tribunal will hear proceedings regarding investigatory activities and regarding loss occasioned by a failure to keep safe a key that has been disclosed and other proceedings allocated to it under the Law.

The Home Affairs Committee will be empowered to issue codes of practice regarding the exercise of investigatory powers. The Codes will be given effect by Order. A person exercising powers or performing duties must have regard to a code of practice and the code will be admissible in evidence in proceedings and must be taken into account, if relevant.

Part 6 – Supplemental

This would make provision for liability for officers and directors of bodies corporate and for amendments and repeals which will be detailed in the Schedules for delegations of certain functions under the Law, as well as various other miscellaneous provisions.

Financial and manpower resource implications

There should not be any need for additional manpower resources in the States of Jersey Police or the Civil Service

as a result of the enactment of the Law. However, it is possible that the extra functions placed upon the Attorney General in granting authorisations will give rise to extra expenditure by, and place extra pressure on, the Law Officers' Department. However, the number of extra warrants or authorisations that may need to be granted will probably be fairly limited.

The Attorney already performs a similar function under the Interception of Communications Law. It will also be possible for the Attorney to ease the extra burden by using the power under the Law to delegate functions to a Crown Advocate. Nevertheless, the effect of the introduction of the Law on the work of the Law Officers' Department will need to be monitored and the need to make provision for extra resources as a result cannot be ruled out. It should be noted that Article 62 of the Law would require the States to provide for any expenditure by the Attorney General under the Law.

The Investigatory Powers commissioner will, in effect take the place of the Interception of Communications Commissioner appointed under the 1993 Law, so there will be no immediate need for an extra appointment. The same applies in relation to the Investigatory Powers Tribunal. However, it is likely that the Commissioner and the Investigatory Powers Tribunal will have to deal with more matters, under the broadened jurisdiction they will have under the new Law to review the exercise of powers given by the Law and to deal with complaints. This could result in increased expenditure by the Commissioner and the Tribunal, though the amounts are very hard to predict. The Tribunal will, like the Interception of Communications Tribunal, have power to award compensation in cases where a complaint is upheld. The current Tribunal has not yet made any award of compensation or indeed been called upon to consider any complaints under the 1993 Law.

There is power to appoint a person with judicial experience as an assistant Commissioner under Part 5 of the Law. This would be an extra appointment, with costs implications, but it is felt that, in the short term anyway, there is not likely to be a need to appoint an assistant.

At some stage in the future, the States may also be required to contribute to the costs incurred by public postal and telecommunications service providers, who are required by the Home Affairs Committee to maintain equipment to carry out intercepts and to provide telecommunications data. The costs of intercepts under the 1993 Law are borne by the public purse since the only public service providers are owned or controlled by the States. In future, licences for public service providers may be granted to private companies as well and some contribution to costs may be necessary to avoid licensees being placed at a competitive disadvantage. Unfortunately, it is impossible to predict accurately, either, when this might occur or the costs involved.

European Convention on Human Rights

Article 16 of the Human Rights (Jersey) Law 2000 will, when brought into force by Act of the States, require the Committee in charge of a Projet de Loi to make a statement about the compatibility of the provisions of the Projet with the Convention rights (as defined by Article 1 of the Law). Although the Human Rights (Jersey) Law 2000 is not yet in force, on 19th June 2003 the Home Affairs Committee made the following statement before Second Reading of this projet in the States Assembly –

In the view of the Home Affairs Committee the provisions of the Draft Regulation of Investigatory Powers (Jersey) Law 200- are compatible with the Convention Rights.

Explanatory Note

This draft Law regulates the interception of communications and the use of surveillance. The Law also makes provision for the decryption of lawfully obtained electronic data, for the appointment of an Investigatory Powers Commissioner to scrutinize the exercise of powers conferred by this Law and for the appointment of an Investigatory Powers Tribunal.

The Law is divided into 6 Parts –

Part 1 contains interpretive material.

Part 2 is in 2 Chapters. *Chapter 1* regulates the interception of communications sent through the post or a telecommunications system. *Chapter 2* confers powers to collect information regarding such communications.

Part 3 regulates the use of covert surveillance.

Part 4 confers powers to have encrypted information rendered in intelligible form.

Part 5 provides for the appointment and functions of the Investigatory Powers Commissioner and the Investigatory Powers Tribunal.

Part 6 contains supplemental provisions.

Part 1 - Introductory

Article 1 is the general interpretation provision.

Article 2 defines "interception", in relation to communications.

Paragraph (2) has the effect that a reference in the Law to the interception of a communication does not include the interception of a television or radio signal but does include pager and mobile phone signals.

Paragraph (3) is concerned with the territorial extent of the Law. The conduct constituting the interception must take place in Jersey.

Article 3 defines "traffic data". The term has particular relevance to Chapter 2 of Part 2, which is concerned with obtaining and disclosing communications data. "Traffic data" includes subscriber information, routing information, data entered in order to effect the re-routing of a telephone call and the data which indicates which communication the traffic data relates to. The closing words of paragraph (1) have the effect that, in the case of internet communications, the traffic data may identify a server but not a website or page.

Part 2 - Communications: Chapter 1 - Interception

Article 4 contains interpretive material for the purposes of Chapter 1.

Article 5 creates 2 offences and regulates requests by a person in Jersey to another country or territory for interception of a communication.

Paragraph (1) makes it an offence to intercept intentionally and without lawfully authority a communication sent through a public postal service or a public telecommunications system. This replaces the offence in Article 2 of the Interception of Communications (Jersey) Law 1993 (the "1993 Law").

Paragraph (2) creates a new offence of intercepting intentionally and without lawfully authority a communication sent through a private telecommunications system. Paragraph (3) creates an exception to the offence where the interception is by or with the consent of the person having the right to control the operation or use of the system. The exception would cover, for example, a individual using a second handset in a house to monitor a telephone call and a financial institution recording calls from the public, in order to retain a record of transactions. However, a civil right of action may arise under Article 6 in respect of the interception.

Paragraph (3) requires the Attorney General to ensure that, where a person in Jersey makes a request for assistance to another country or territory pursuant to an international mutual assistance agreement, the request has lawful authority. Currently, there are no international mutual assistance agreements applicable to Jersey but provision is included for them to provide flexibility for the future.

The penalty for an offence under this Article is imprisonment for up to 2 years and/or an unlimited fine.

Article 6 creates a civil right of action for the sender or recipient of a communication sent by means of a private telecommunications system which is intercepted without lawful authority and without the express or implied consent of a person having control of the system.

Article 7 summarizes the circumstances in which an interception has lawful authority.

Article 8 describes circumstances in which a communication can be intercepted lawfully without the need for an interception warrant. Interception is lawful –

if both the sender and recipient have or are believed to have consented;

if either the sender or the recipient has consented and the interception has been authorized under Part 3 (an example of this would be where a kidnapper telephones the relatives of a hostage and the relatives consent to interception by the police in order to identify or trace the kidnapper, in which case the interception is authorized as surveillance under Part 3);

if the interception is by the person providing the postal or telecommunications service and is either connected with the provision of the service or for the enforcement of legislation relating to the service (an example would be a postal provider opening a letter to determine the sender's address, because the recipient's address is unknown);

if the communication is intercepted whilst being transmitted by wireless telegraphy and the interception is authorized under the Wireless Telegraphy Act 1949, as it has effect in Jersey, or for other purposes connected with that Act.

Article 9 describes cases where a power may be exercised to provide for lawful interception without an interception warrant.

Paragraph (1) authorizes the interception of communications of a person believed to be outside Jersey, but would not be effective unless the Home Affairs Committee (the "Committee") made an Order imposing conditions as to when conduct may be treated as authorized by the paragraph. There must be lawful authority for the interception in force in the country or territory where the person is believed to be. The conduct authorized would be the use of a telecommunications system in Jersey to intercept the person's communications in accordance with that lawful authority. In practice, the interception is likely to be by a communication service provider in Jersey which is either providing a public telecommunications service to another country or is in a business relationship with another communication service provider providing such a service.

Paragraphs (2) and (3) enable the Committee to make an Order authorizing interceptions in the course of legitimate business practice (including the business of States' departments and other public authorities). An example would be the monitoring of calls made to a call centre, provided that steps are taken to ensure the caller is made aware that such monitoring may occur.

Paragraph (4) authorizes any interception conducted in accordance with Rules made under the Prison (Jersey) Law 1957.

Article 10 describes when the Attorney General may issue a warrant –

(a) authorizing the interception of a communication in Jersey and the disclosure of the intercepted material; or

(b) authorizing the making of a request to another country or territory for an interception under an international mutual assistance agreement.

The grounds for issuing a warrant are that it is in the interests of national security, for the purpose of preventing or detecting serious crime, to safeguard the economic well-being of Jersey (but only where the information to be obtained relates to the acts or intentions of persons outside Jersey) or to assist another country or territory in the prevention or detection of serious crime.

Article 11 states who can apply for an interception warrant. An application can be made only by the Chief Officer of the States of Jersey Police, the Agent of the Impôts, the Chief Inspector of Immigration, the Director General of the Security Services, the Chief of the Secret Intelligence Services, the Director of GCHQ, the Chief of Defence Intelligence within the Ministry of Defence and any person who, for the purposes of an international mutual assistance agreement, is the competent authority of another country or territory.

Article 12 states the required contents of an interception warrant. The warrant must relate to either a named person as the interception subject or to a single set of premises. The warrant must have a schedule which lists the addresses, numbers, email addresses and equipment by which the communications which may be intercepted are to be identified (the "identifying factors"). There is an exception to these requirements if the warrant relates only to the interception of communications sent or received outside Jersey and the Attorney General has given a certificate (an "Article 12(4) certificate") of the descriptions of information to be intercepted and the grounds for interception.

Article 13 provides that an interception warrant initially has effect and, after that, may be renewed for 3 months, save that a warrant issued in the interests of national security or to safeguard the economic well-being of Jersey may be renewed for 6 months. The Attorney General must cancel a warrant at any time when the grounds for interception cease to be satisfied.

Article 14 enables the Attorney General to modify a warrant. If the warrant so provides, the warrant may, in an emergency, be modified by the person to whom it is addressed.

Article 15 describes how an interception warrant is implemented. The person to whom the warrant is addressed must give effect to it, but may require others to provide assistance by serving a copy of the warrant on them, or a copy of so much of the warrant as authorizes the actions to be taken by the other persons. A person is not required to assist if it is not reasonably practicable for that person to assist but, otherwise, failure to comply is an offence liable to imprisonment for up to 2 years and/or a fine. The Attorney General may take injunctive proceedings to enforce the duty.

Article 16 empowers the Committee to make an Order under which the Committee may give the providers of public postal services and public telecommunications services notice requiring them to maintain interception capabilities. The Committee must consult with interested parties before making the Order. A provider who is given notice can refer the notice to the Technical Advisory Board established under Article 17. The Board must then consider the technical and financial consequences of the notice for the provider and report upon those consequences to the Committee. The duty to maintain interception capabilities may be enforced by injunctive proceedings taken by the Attorney General.

Article 17 establishes the Technical Advisory Board. The Board members are appointed by the Committee, which is required to ensure that there is equal representation of the interests of providers of public postal services and public telecommunications services and of the persons who may apply for warrants.

Article 18 imposes a duty on the States to ensure that arrangements are in place for contributions to be paid out of the annual income of the States towards the costs incurred by providers of public postal services and public telecommunications services in complying with an obligation to maintain an interception capability.

Article 19 requires the Attorney General to make arrangements in order to secure that intercepted material is distributed and disclosed to the minimum number of people necessary, to restrict the copying of intercepted material, to require its destruction once there are no longer grounds for retaining it and for its secure storage.

Article 20 imposes additional requirements in the case of a warrant accompanied by an Article 12(4) certificate. It limits the circumstances in which the material may be read or listened to. Broadly, the material may only be read or listened in the interests of national security, to prevent or detect serious crime or to safeguard the economic well-being of Jersey and should not relate to an individual in Jersey, although the Attorney General can give a certificate whereby communications relating to an individual in Jersey and sent over a period of up to 3 months may be read or listened to. If there is a change of circumstances, in that the individual enters or is found to be in Jersey, the Attorney General may authorize the reading of or listening to material selected within one working day of the change in circumstances.

Article 21 restricts the use in evidence in civil or criminal proceedings of any information that might indicate that an interception warrant has been issued, that a communication has been intercepted either pursuant to an interception warrant or, unlawfully, by a person to whom a warrant may be issued or that a person has been required to assist with giving effect to a warrant. It replaces Article 10 of the 1993 Law.

Article 22 contains exceptions to the restriction in Article 21. The principal exceptions are for material intercepted lawfully by virtue of Article 7(c), 8 or 9 of this Law, for criminal proceedings for an offence under this Law or other enactments regarding interception and for proceedings before the Tribunal established under this Law. In addition, the Bailiff can order the disclosure of information to the Bailiff alone, in the interests of justice. Having heard the disclosure, the Bailiff can require the prosecution to make any admission of fact (other than an

admission tending to suggest that an interception has taken place) that the Bailiff considers essential in the interests of justice.

Article 23 imposes a duty on persons whose office or employment may give them knowledge of the existence of an interception warrant or of the contents of an intercepted communication to keep that knowledge secret. Disclosure to any other person is an offence for which the penalty is 5 years imprisonment and an unlimited fine. There is a defence where the disclosure could not reasonably have been prevented, for legal professional privilege and where disclosure is to the Commissioner appointed under this Law or required by or under the terms of the interception warrant.

Part 2 - Communications: Chapter 2 - Acquisition and disclosure of communications data

Article 24 is the interpretation provision for Chapter 2. It defines "communications data", which is information regarding the sender and recipient of communications (whether postal or telecommunications), dates and times of communications and equipment used. "Communications data" does not include the contents of the communication.

Article 25 makes it lawful to obtain and disclose communications data pursuant to an authorization or notice given under this Chapter by a designated person to a relevant public authority. Designated persons and their relevant public authorities are listed in Schedule 1.

Article 26 confers the power to grant authorizations and give notices. The designated person for a public authority may grant authorizations to officers of that authority to obtain communications data. If the communications could be obtained by or is already in the possession of a postal or telecommunications operator, the designated person can give a notice requiring the operator to obtain or release the data. The operator's duty to comply with the notice may be enforced by injunctive proceedings taken by the Attorney General. An authorization or notice may be given in the interests of national security, to prevent or detect crime or to prevent disorder, in the interests of the economic well-being of Jersey, in the interests of public safety, to protect public health, in order to assess or collect any tax, duty or other charge payable to the States or an administration of the States, to prevent or mitigate any injury or damage to an individual's health or for any other purpose that may be specified in Regulations made by the States.

Article 27 specifies the information that must be obtained in an authorization or notice and limits disclosure of data obtained pursuant to a notice to officers and employees of the authority for whose purposes the notice is given. An authorization or notice takes effect for one month, and may be renewed. The designated person must cancel the authorization or notice if it is no longer necessary on the grounds described in Article 26 or if the conduct required by it has become disproportionate to what is to be achieved.

Article 28 imposes a duty on the States to contribute, out of public funds, to the costs incurred by postal and telecommunications operators in complying with notices.

Article 29 gives effect to Schedule 1, in which designated persons and relevant public authorities are listed for the purpose of this Chapter. The States are given power, by Regulations, to add any public authority in Jersey to Schedule 1 and a limited power to add certain public authorities outside Jersey. Only the Attorney General can be the designated person in relation to a public authority outside Jersey.

Part 3 - Surveillance and covert human intelligence sources

Articles 30 to 32 contain interpretive material for Part 3 and, in particular, define the 3 types of covert surveillance to be regulated -

> "Directed surveillance" is surveillance which is covert, but not intrusive, carried out for a specific investigation or operation and likely to result in obtaining private information about a person. An example would be maintaining a watch on a person's residence.
>
> "Intrusive surveillance" is covert surveillance of anything happening in residential premises or in a private vehicle, either by means of an individual on the premises or in the vehicle or by means of a surveillance device. The device must be on the premises or in the vehicle, unless it is capable of providing the same information, when located externally, as might be obtained from a device actually on the premises or in the vehicle. Intrusive surveillance does not include the use of a vehicle tracking device or the interception of communications.

"Covert human intelligence source" is the use or conduct of an individual who establishes or maintains a relationship with a person in order to obtain information about that person, without that person being aware of the purpose for which the information is obtained or the use to which it will be put.

Article 33 makes it lawful to conduct any of these 3 forms of surveillance in accordance with an authorization under this Part.

Article 34 empowers a designated person to authorize the conduct of directed surveillance by the public authority in relation to which that person is designated. The designated persons and their public authorities are listed in Parts 1 and 2 of Schedule 2. An authorization may be given in the interests of national security, to prevent or detect crime or prevent disorder, in the interests of the economic well-being of Jersey, in the interests of public safety or to protect public health, in order to assess or collect any tax, duty or other charge payable to the States or an administration of the States and for any other purpose specified in Regulations made by the States. The surveillance to be carried out must be proportionate to what is to be achieved and the authorization must specify the investigation or operation for which the surveillance is to be carried out.

Article 35 empowers a designated person to authorize the use of a covert human intelligence source by the public authority in relation to which that person is designated. The designated persons and their public authorities are listed in Part 1 of Schedule 2. The grounds for use of such a source are the same as those for the use of directed surveillance but there are additional requirements concerning the use of the source. There must be an officer in the public authority who has day to day responsibility for contact with the source and the source's welfare. There must be another officer who oversees the use of the source. A record must be maintained of the use of the source and contain any particulars prescribed by Order of the Committee. There must be restricted access to details of the source's identity.

Article 36 gives effect to Schedule 2. The designated persons in Part 1 of Schedule 2 can authorize directed surveillance and the use of covert human intelligence sources. The designated persons in Part 2 of Schedule 2 can only authorize directed surveillance. The States may amend Schedule 2 by Regulations but, by virtue of the definition "public authority" in Article 1, the only authorities outside Jersey that may be included in the Schedule are the intelligence services, the Ministry of Defence of the United Kingdom and Her Majesty's Forces.

Article 37 empowers the Attorney General to authorize intrusive surveillance. Only the Chief Officer of the States of Jersey Police, the Agent of the Impôts, the Chief Inspector of Immigration, a member of the intelligence services, an official of the Ministry of Defence of the Government of the United Kingdom or a member of Her Majesty's Forces can apply for an authorization. An authorization can only be given in the interests of national security, to prevent or detect serious crime or in the interests of the economic well-being of Jersey. A member of the intelligence services, an official of the Ministry of Defence of the Government of the United Kingdom or a member of Her Majesty's Forces cannot make an application in the interests of the economic well-being of Jersey. The surveillance must be proportionate to what is to be achieved by it. The Attorney General must consider whether the information to be obtained could be reasonably obtained by other means. The authorization must specify the investigation or operation for which the surveillance is to be carried out.

Article 38 makes it clear that a person empowered to authorize directed surveillance or the use of a covert human intelligence source can only give an authorization to a member of the organization in relation to which he or she is designated. The Attorney General is empowered to combine an authorization under this Part and an authorization under Article 101 of the Police Procedures and Criminal Evidence (Jersey) Law 2003. Article 101 empowers the Attorney General to authorize any act in relation to property or wireless telegraphy as is necessary to prevent or detect serious crime or in the interests of the security of Jersey. The act must be proportionate to what is to be achieved.

Article 39 requires the Attorney General to notify the Investigatory Powers Commissioner, at least every 12 months, of authorizations for intrusive surveillance granted, renewed or cancelled.

Article 40 contains general provisions regarding authorizations under this Part. A single authorization may combine 2 or more different authorizations under this Part. An authorization granted or renewed orally has effect for 72 hours. The grant or renewal of a written authorization to use a covert human intelligence source has effect for 12 months. The grant or renewal of a written authorization for directed or intrusive surveillance has effect for 3 months. The Committee has power to shorten these periods by Order.

Article 41 requires a person who has given an authorization to cancel it once there are no longer grounds for it or if, in the case of a covert human intelligence source, the additional arrangements required by Article 35 are no longer in place.

Article 42 empowers the States to make Regulations extending Part 3 to surveillance that is neither directed or intrusive and providing for any particular description of directed surveillance to be subject to the more restrictive rules for authorization of intrusive surveillance.

Part 4 - Investigation of electronic data protected by encryption

Part 4 confers powers where information in the format of electronic data which 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 43 is the general interpretation provision for Part 4.

Article 44 confers the right to give a notice (an "Article 44 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 3, 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 45 describes the effect of an Article 44 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 46 is concerned with Article 44 notices which can only be complied with 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 only be given if there are special circumstances which mean that, if the direction were not given, the purposes of the requirement for disclosure would be defeated and if 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, the Agent of the Impôts or the Chief Inspector of Immigration.

Article 47 imposes a duty on the States to ensure that a contribution is made out of public funds to the costs incurred by persons complying with Article 44 notices.

Article 48 makes it an offence to fail to comply with an Article 44 notice for which the penalty is imprisonment for 2 years and 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 by merely 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 49 firstly enables a person giving an Article 44 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 44 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, Customs and Excise, the Immigration and Nationality Department 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 44 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 50 imposes duties on the Attorney General, States Committees, the Chief Officer of the States of Jersey Police, the Agent of the Impôts, the Chief Inspector of Immigration and ever other person whose officers and employees include duties include giving Article 44 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.

Part 5 - Scrutiny etc. of investigatory powers

Part 5 is concerned with overseeing and scrutinizing the use of investigatory powers.

Article 51 requires the Bailiff to appoint one of the ordinary judges of the Court of Appeal as the Investigatory Powers Commissioner. The Commissioner's duty is to review the exercise and performance of all powers conferred and duties imposed by the Law, and assist the Investigatory Powers Tribunal as required. It is proposed that the person appointed as Commissioner under Article 9 of the 1993 Law shall, on the repeal of that Law and coming into force of this Law, become the Investigatory Powers Commissioner.

Article 52 imposes duties. Officers and employees having powers under this Law and persons required, pursuant to any notice or authorization under this Law, to disclose information, must disclose such information to the Commissioner as he or she requires in the discharge of the Commissioner's functions. The Commissioner must report to the Bailiff if the Commissioner suspects any contravention of the Law or that inadequate arrangements have been made to safeguard intercepted material and keys from disclosure. The Commissioner must also report annually to the Bailiff on the discharge of his or her functions. The Bailiff must lay a copy of the Commissioner's report before the States, but has a power to omit from it any material that might be contrary to public interest or prejudicial to national security, preventing or detecting serious crime, the economic well-being of Jersey or the continued discharge of a public authority' functions.

Article 53 empowers the Bailiff to appoint Assistant Commissioners to assist the Commissioner. The appointee must be a present or past judge of the Royal Court or of a court of comparable authority elsewhere in the British Islands.

Article 54 establishes the Investigatory Powers Tribunal. The Tribunal consists of 3 members appointed by the Superior Number of the Royal Court: an ordinary judge of the Court of Appeal, who is to preside, and 2 Jurats. Broadly, the Tribunal's jurisdiction is to hear –

> proceedings concerning actions of the intelligence services which are incompatible with the European Convention on Human Rights;
>
> proceedings concerning investigatory powers regulated by this Law or entry on or interference with property or wireless telegraphy conducted by public authorities;
>
> complaints by a person who believes he or she has been subject to the use of investigatory powers, entry on or interference with property or interference with wireless telegraphy, in certain challengeable circumstances;
>
> complaints by a person that he or she has suffered detriment as a consequence of a breach of the duty to keep a key to protected information secure.

Article 55 makes further provision as to the contents of Orders allocating proceedings to the Tribunal.

Article 56 requires the Tribunal to determine proceedings in which they have jurisdiction and apply the same principles in doing so as would be applied on a judicial review. The Tribunal, in determining any proceedings or complaint can make such order as they think fit, including an order for compensation.

Article 57 provides that, subject to rules made under Article 58, the Tribunal may determine their own procedures The Tribunal can require the Investigatory Powers Commissioner to provide them with assistance and are required to keep the Commissioner informed of proceedings before them. If the Tribunal makes a determination in favour of a complainant which relates to an act or omission on behalf of the Attorney General or to conduct for which the Attorney General has given any warrant, authorization or permission, the Tribunal must report their finding to the Bailiff. The persons who are under a duty to provide information to the Commissioner under

Article 52 are also under a like duty to provide information to the Tribunal.

Article 58 empowers the Bailiff to make rules regarding the procedures of the Tribunal.

Article 59 empowers the Committee to bring into force codes of practice regarding the powers and duties conferred by the Law and the Attorney General's power to issue warrants authorizing entry on or interference with property or interference with wireless telegraphy under Article 101 of the Police Procedures and Criminal Evidence (Jersey) Law 2003. The Committee must publish the codes in draft form and consider representations on them before bringing them into force by Order. It is envisaged that codes will be brought into force regarding the interception of communications, intrusive surveillance and the use of covert human intelligence sources.

Article 60 describes the effect of a code of practice. A person exercising a power or performing a duty must have regard to the code. Failure to do so is not an offence, but the code is admissible in criminal or civil proceedings and a court, the Investigatory Powers Tribunal and the Commissioner must take the code into consideration when it is relevant to any proceedings or in the discharge of any functions.

Article 61 empowers the Attorney General to delegate to the Solicitor General or a Crown Officer any power to give an authorization or notice for the disclosure of communications data, directed surveillance or the use of a covert human intelligence source.

Part 6 - Supplemental

Article 62 imposes a duty on the States to fund expenditure incurred by the Attorney General in the discharge of the Attorney General's functions under the Law, expenditure incurred by the Committee in the discharge of the Committee's functions under the Law and any increase in the amounts payable under any other enactment which is attributable to this Law.

Article 63 empowers the Committee to prescribe by Order anything that shall or may be prescribed under this Law.

Article 64 is the standard provision for offences by bodies corporate and partnerships.

Article 65 makes it clear that the Law does not operate so as to make unlawful any conduct which is otherwise lawful.

Article 66 gives effect to Schedule 5, which contains consequential amendments to other enactments, repeals the Interception of Communications (Jersey) Law 1993, and contains transitional provisions relating to that repeal

Article 67 is the citation and commencement provision.

Schedule 1 lists designated persons and the relevant public authorities for which they can give authorizations to obtain communications data.

Schedule 2 relates to surveillance. Part 1 lists designated persons and the public authorities for which they can give authorizations to use directed surveillance and covert human intelligence sources. Part 2 lists designated persons and the public authorities for which they can give authorizations to use directed surveillance only.

Schedule 3 describes what constitutes the appropriate permission to give an Article 44 notice requiring the use or disclosure of a key for the decryption of protected information.

Schedule 4 contains further provision regarding the constitution of the Investigatory Powers Tribunal.

Schedule 5 contains amendments of other enactments. The amendments are directly consequential upon the enactment of this Law, with the exception of one amendment to the Police Procedures and Criminal Evidence (Jersey) Law 2003. Currently, any person may apply to the Attorney General for an authorization to interfere with property under Article 101 of that Law. That provision is amended so as to limit the persons who may apply to the Attorney General under it to the persons who may apply for an authorization of intrusive surveillance under Article 37 of this Law.

Under the Criminal Justice (Standard Scale of Fines) (Jersey) Law 1994, level 1 is £50, level 2 is £500, level 3 is £2,000 and level 4 is £5,000.

The Interpretation (Amendment) (Jersey) Law 2003 which came into force on 28th March 2003 has the effect that –

(a) where a penalty is specified for an offence, the offence is punishable by a penalty not exceeding the penalty specified;

(b) where the penalties for an offence are stated to be a term of imprisonment and a fine, either or both of the penalties may be imposed.

Jersey

DRAFT REGULATION OF INVESTIGATORY POWERS (JERSEY) LAW 200-

Arrangement

Article

Jersey

DRAFT REGULATION OF INVESTIGATORY POWERS (JERSEY) LAW 200-

A LAW to regulate the interception of communications and the use of surveillance; to confer powers to require the decryption of certain data; 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 –

PART 1

INTRODUCTORY

1 Interpretation

(1) In this Law, unless the context otherwise requires –

"1949 Act" means the Wireless Telegraphy Act 1949 of the United Kingdom as extended to Jersey by the Wireless Telegraphy (Channel Islands) Order 1952;[1]

"1994 Act" means the Intelligence Services Act 1994 as extended to Jersey by the Intelligence Services Act 1994 (Channel Islands) Order 1994;[2]

"Agent of the Impôts" means the person appointed as such under Article 4 of the Customs and Excise (Jersey) Law 1999[3] and includes any Deputy Agent of the Impôts so appointed;

"apparatus" includes any equipment, machinery or device and any wire or cable;

"Assistant Commissioner" means an Assistant Investigatory Powers Commissioner appointed under Article 53(1);

"Chief Inspector of Immigration" means the most senior immigration officer;

"Chief Officer" means the Chief Officer of the Force appointed under Article 9 of the Police Force (Jersey) Law 1974[4] and includes the Deputy Chief Officer so appointed;

"civil proceedings" means any proceedings in or before any court or tribunal that are not criminal proceedings;

"Commissioner" means the Investigatory Powers Commissioner appointed under Article 51(1);

"Committee" means the Home Affairs Committee;

"communication" includes –

(a) (except in the definition of "postal service") anything transmitted by means of a postal service;

(b) anything comprising speech, music, sounds, visual images or data of any description; and

(c) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus;

"crime" means conduct which constitutes one or more criminal offences or is, or corresponds to, any conduct which, if it all took place in Jersey, would constitute one or more criminal offences;

"Customs and Excise" means the Agent of the Impôts and officers of the Impôts;

"document" includes a map, plan, design, drawing, picture or other image;

"enactment" means any enactment, whenever passed;

"Force" means the States of Jersey Police Force;

"GCHQ" means the Government Communications Headquarters continued under section 3 of the 1994 Act;

"Immigration and Nationality Department" means the immigration officers;

"immigration officer" means an officer appointed under paragraph 1(1) of Part 1 of Schedule 2 to the Immigration Act 1971as extended to Jersey by the Immigration (Jersey) Order 1993;[5]

"interception" and cognate expressions shall be construed (so far as it is applicable) in accordance with Article 4;

"interception warrant" means a warrant under Article 10;

"intelligence services" means –

(a) the Secret Intelligence Service;

(b) GCHQ;

(c) the Security Service;

"legal proceedings" means civil or criminal proceedings in or before any court or tribunal;

"modification" includes alterations, additions and omissions, and cognate expressions shall be construed accordingly;

"officer of the Impôts" shall be construed in accordance with Article 4 of the Customs and Excise (Jersey) Law 1999;[6]

"police officer" means a member of the Force or of the Honorary Police;

"person" includes any organization and any association or combination of persons;

"postal item" means any letter, postcard or other such thing in writing as may be used by the sender for imparting information to the recipient, or any packet or parcel;

"postal service" means any service which –

(a) consists in the following, or in any one or more of them, namely, the collection, sorting, conveyance, distribution and delivery (whether in Jersey or elsewhere) of postal items; and

(b) is offered or provided as a service the main purpose of which, or one of the main purposes of which, is to make available, or to facilitate, a means of transmission from place to place of postal items containing communications;

"prescribed" means prescribed by Order of the Committee;

"private telecommunication system" means any telecommunication system which, without itself

being a public telecommunication system, is a system in relation to which the following conditions are satisfied –

(a) it is attached, directly or indirectly and whether or not for the purposes of the communication in question, to a public telecommunication system; and

(b) there is apparatus comprised in the system which is both located in Jersey and used (with or without other apparatus) for making the attachment to the public telecommunication system;

"Proscribed Organizations Appeal Commission" has the same meaning as in the Terrorism (Jersey) Law 2002;[7]

"public authority" means any public authority within the meaning of Article 7 of the Human Rights (Jersey) Law 2000[8] other than a court or tribunal and includes –

(a) any of the intelligence services;

(b) the Ministry of Defence of the Government of the United Kingdom;

(c) Her Majesty's Forces,

and further includes, in Chapter 2 of Part 2 and in Part 5, to the extent that Part 5 applies to acts regulated, powers conferred and duties imposed by Chapter 2 of Part 2, any other public authority outside Jersey specified pursuant to Article 29;

"public postal service" means any postal service which is offered or provided to, or to a substantial section of, the public in any one or more parts of Jersey;

"public telecommunications service" means any telecommunications service which is offered or provided to, or to a substantial section of, the public in Jersey;

"public telecommunication system" means any such parts of a telecommunication system by means of which any public telecommunications service is provided as are located in Jersey;

"Secret Intelligence Service" means the service continued under section 1 of the 1994 Act;

"Security Service" means the service continued by section 1 of the Security Service Act 1989 of the United Kingdom Parliament;

"serious crime" means conduct which constitutes one or more offences –

(a) which involves the use of violence, results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose; and

(b) for which a person who has attained the age of 21 and has no previous convictions could reasonably be expected to be sentenced to imprisonment for 3 years or more;

"statutory", in relation to any power or duty, means conferred or imposed by or under any enactment;

"Technical Advisory Board" shall be construed in accordance with Article 17;

"telecommunications service" means any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service);

"telecommunication system" means any system (including the apparatus comprised in it) which exists (whether wholly or partly in Jersey or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy;

"traffic data" has the meaning given in Article 3;

"Tribunal" means the Investigatory Powers Tribunal established under Article 54(1);

"wireless telegraphy" has the same meaning as in the 1949 Act and, in relation to wireless telegraphy, "interfere" has the same meaning as in that Act;

"working day" means any day other than a Saturday, a Sunday, Christmas Day, Good Friday or a day

which is observed as a bank holiday pursuant to the Public Holidays and Bank Holidays (Jersey) Law 1951[9]

(2) For the purposes of this Law detecting crime shall be taken to include –

(a) establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed; and

(b) the apprehension of the person by whom any crime was committed,

and any reference in this Law to preventing or detecting serious crime shall be construed accordingly, except that, in Chapter 1 of Part 2, it shall not include a reference to gathering evidence for use in any legal proceedings.

2 Meaning and location of "interception" etc.

(1) For the purposes of this Law, but subject to the following provisions of this Article, a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, that person –

(a) so modifies or interferes with the system, or its operation;

(b) so monitors transmissions made by means of the system; or

(c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system,

as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication.

(2) References in this Law to the interception of a communication do not include references to the interception of any communication broadcast for general reception.

(3) For the purposes of this Law the interception of a communication takes place in Jersey if, and only if, the modification, interference or monitoring or, in the case of a postal item, the interception is effected by conduct within Jersey and the communication is either –

(a) intercepted in the course of its transmission by means of a public postal service or public telecommunication system; or

(b) intercepted in the course of its transmission by means of a private telecommunication system in a case in which the sender or intended recipient of the communication is in Jersey.

(4) References in this Law to the interception of a communication in the course of its transmission by means of a postal service or telecommunication system do not include references to –

(a) any conduct that takes place in relation only to so much of the communication as consists in any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted; or

(b) any such conduct, in connection with conduct falling within sub-paragraph (a), as gives a person who is neither the sender nor the intended recipient only so much access to a communication as is necessary for the purpose of identifying traffic data so comprised or attached.

(5) For the purposes of this Article references to the modification of a telecommunication system include references to the attachment of any apparatus to, or other modification of or interference with –

(a) any part of the system; or

(b) any wireless telegraphy apparatus used for making transmissions to or from apparatus comprised in the system.

(6) For the purposes of this Article the times while a communication is being transmitted by means of a telecommunication system shall be taken to include any time when the system by means of which the

communication is being, or has been, transmitted is used for storing it in a manner that enables the intended recipient to collect it or otherwise to have access to it.

(7) For the purposes of this Article the cases in which any contents of a communication are to be taken to be made available to a person while being transmitted shall include any case in which any of the contents of the communication, while being transmitted, are diverted or recorded so as to be available to a person subsequently.

3 Meaning of "traffic data", etc.

(1) In this Law "traffic data", in relation to any communication, means –

(a) any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted;

(b) any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted;

(c) any data comprising signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of any communication; and

(d) any data identifying the data or other data as data comprised in or attached to a particular communication,

but that expression includes data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored.

(2) In this Law –

(a) references, in relation to traffic data comprising signals for the actuation of apparatus, to a telecommunication system by means of which a communication is being or may be transmitted include references to any telecommunication system in which that apparatus is comprised; and

(b) references to traffic data being attached to a communication include references to the data and the communication being logically associated with each other.

(3) In this Article, "data", in relation to a postal item, means anything written on the outside of the item.

PART 2

COMMUNICATIONS

CHAPTER 1

INTERCEPTION

4 Interpretation of Chapter 1

In this Chapter –

"certified", in relation to an Article 12(4) certificate, means of a description certified by the certificate as a description of material the examination of which the Attorney General considers necessary;

"intercepted material", in relation to an interception warrant, means the contents of any communications intercepted by an interception to which the warrant relates;

"interception subject", in relation to an interception warrant, means the person about whose

communications information is sought by the interception to which the warrant relates;

"international mutual assistance agreement" means an international agreement designated for the purposes of Article 5(4);

"related communications data", in relation to a communication intercepted in the course of its transmission by means of a postal service or telecommunication system, means so much of any communications data (within the meaning of Chapter 2 of this Part) as –

(a) is obtained by, or in connection with, the interception; and

(b) relates to the communication or to the sender or recipient, or intended recipient, of the communication;

"Article 12(4) certificate" means any certificate issued for the purposes of Article 12(4).

5 Unlawful interception

(1) It shall be an offence for a person intentionally and without lawful authority to intercept, at any place in Jersey, any communication in the course of its transmission by means of –

(a) a public postal service; or

(b) a public telecommunication system.

(2) It shall be an offence for a person –

(a) intentionally and without lawful authority; and

(b) otherwise than in circumstances in which the person's conduct is excluded by paragraph (3) from criminal liability under this paragraph,

to intercept, at any place in Jersey, any communication in the course of its transmission by means of a private telecommunication system.

(3) The circumstances in which a person makes an interception of a communication in the course of its transmission by means of a private telecommunication system are such that the person's conduct is excluded from criminal liability under paragraph (2) if the person has–

(a) a right to control the operation or the use of the system; or

(b) the express or implied consent to make the interception of another person having a right to control the operation or the use of the system.

(4) Where Jersey is a party to an international agreement which –

(a) relates to the provision of mutual assistance in connection with, or in the form of, the interception of communications;

(b) requires the issue of a warrant, order or equivalent instrument in cases in which assistance is given; and

(c) is designated for the purposes of this paragraph by an Order made by the Committee,

the Attorney General shall secure that no request for assistance in accordance with the agreement is made on behalf of a person in Jersey to the competent authorities of a country or territory outside Jersey except with lawful authority.

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

(6) No proceedings for any offence which is an offence by virtue of this Article shall be instituted except by or with the consent of the Attorney General.

6 Civil action in respect of interception

Any interception of a communication which is carried out at any place in Jersey by, or with the express or

implied consent of, a person having the right to control the operation or the use of a private telecommunication system shall be actionable at the suit or instance of the sender or recipient, or intended recipient, of the communication if it is without lawful authority and is either –

(a) an interception of that communication in the course of its transmission by means of that private system; or

(b) an interception of that communication in the course of its transmission, by means of a public telecommunication system, to or from apparatus comprised in that private telecommunication system.

7 Lawful authority for interception

Conduct has lawful authority for the purposes of Articles 5 and 6 if, and only if–

(a) it is authorized by or under Article 8 or 9;

(b) it takes place in accordance with an interception warrant; or

(c) it is in exercise, in relation to any stored communication, of any statutory power that is exercised (apart from this Article) for the purpose of obtaining information or of taking possession of any document or other property,

and conduct (whether or not prohibited by Article 5 or 6) which has lawful authority for the purposes of Articles 5 and 6 by virtue of paragraph (a) or (b) shall also be taken to be lawful for all other purposes.

8 Lawful interception without an interception warrant

(1) Conduct by any person consisting in the interception of a communication is authorized by this Article if the communication is one which, or which that person has reasonable grounds for believing, is both –

(a) a communication sent by a person who has consented to the interception; and

(b) a communication the intended recipient of which has so consented.

(2) Conduct by any person consisting in the interception of a communication is authorized by this Article if –

(a) the communication is one sent by, or intended for, a person who has consented to the interception; and

(b) surveillance by means of that interception has been authorized under Part 3.

(3) Conduct consisting in the interception of a communication is authorized by this Article if –

(a) it is conduct by or on behalf of a person who provides a postal service or a telecommunications service; and

(b) it takes place for purposes connected with the provision or operation of that service or with the enforcement, in relation to that service, of any enactment relating to the use of postal services or telecommunications services.

(4) Conduct by any person consisting in the interception of a communication in the course of its transmission by means of wireless telegraphy is authorized by this Article if it takes place –

(a) with the authority of a designated person under section 5 of the 1949 Act; and

(b) for purposes connected with –

(i) the issue of licences under the 1949 Act,

(ii) the prevention or detection of anything which constitutes interference with wireless telegraphy, or

(iii) the enforcement of any enactment contained in that Act or of any enactment not so contained that relates to such interference.

9 Powers to provide for lawful interception

(1) Conduct by any person (the "interceptor") consisting in the interception of a communication in the course of its transmission by means of a telecommunication system is authorized by this Article if –

(a) the interception is carried out for the purpose of obtaining information about the communications of a person who, or who the interceptor has reasonable grounds for believing, is in a country or territory outside Jersey;

(b) the interception relates to the use of a telecommunications service provided to persons in that country or territory which is either –

(i) a public telecommunications service, or

(ii) a telecommunications service that would be a public telecommunications service if the persons to whom it is offered or provided were members of the public in a part of Jersey;

(c) the person who provides that service (whether the interceptor or another person) is required by the law of that country or territory to carry out, secure or facilitate the interception in question;

(d) the situation is one in relation to which such further conditions as may be prescribed are required to be satisfied before conduct may be treated as authorized by virtue of this paragraph; and

(e) the conditions so prescribed are satisfied in relation to that situation.

(2) Subject to paragraph (3), the Committee may by Order authorize any such conduct described in the Order as appears to it to constitute a legitimate practice reasonably required for the purpose, in connection with the carrying on of any business, of monitoring or keeping a record of –

(a) communications by means of which transactions are entered into in the course of that business; or

(b) other communications relating to that business or taking place in the course of its being carried on.

(3) Nothing in any Order under paragraph (2) shall authorize the interception of any communication except in the course of its transmission using apparatus or services provided by or to the person carrying on the business for use wholly or partly in connection with that business.

(4) Conduct taking place in a prison is authorized by this Article if it is conduct in exercise of any power conferred by or under any rules made under Article 26 of the Prison (Jersey) Law 1957.[10]

(5) In this Article –

(a) references to a business include references to any activities of any administration of the States or of a Committee of the States, of any public authority or of any person or office holder on whom functions are conferred by or under any enactment;

(b) "prison" has the same meaning as in the Prison (Jersey) Law 1957.[11]

10 Power to issue interception warrant

(1) Subject to the following provisions of this Chapter, the Attorney General may issue a warrant authorizing or requiring the person to whom it is addressed, by any such conduct as may be described in the warrant, to secure any one or more of the following –

(a) the interception in the course of their transmission by means of a postal service or telecommunication system of the communications described in the warrant;

(b) the making, in accordance with an international mutual assistance agreement, of a request for the provision of such assistance in connection with, or in the form of, an interception of communications as may be so described;

(c) the provision, in accordance with an international mutual assistance agreement, to the competent authorities of a country or territory outside Jersey of any such assistance in connection with, or in the form of, an interception of communications as may be so described;

(d) the disclosure, in such manner as may be so described, of intercepted material obtained by any interception authorized or required by the warrant, and of related communications data.

(2) The Attorney General shall not issue an interception warrant unless the Attorney General believes –

(a) that the warrant is necessary on grounds falling within paragraph (3); and

(b) that the conduct authorized by the warrant is proportionate to what is sought to be achieved by that conduct.

(3) Subject to the following provisions of this Article, a warrant 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 serious crime;

(c) for the purpose of safeguarding the economic well-being of Jersey; or

(d) for the purpose, in circumstances appearing to the Attorney General to be equivalent to those in which the Attorney General would issue a warrant by virtue of sub-paragraph (b), of giving effect to the provisions of any international mutual assistance agreement.

(4) The matters to be taken into account in considering whether the requirements of paragraph (2) are satisfied in the case of any warrant shall include whether the information which it is thought necessary to obtain under the warrant could reasonably be obtained by other means.

(5) A warrant shall not be considered necessary on the ground falling within paragraph (3)(c) unless the information which it is thought necessary to obtain is information relating to the acts or intentions of persons outside Jersey.

(6) The conduct authorized by an interception warrant shall be taken to include –

(a) all such conduct (including the interception of communications not identified by the warrant) as it is necessary to undertake in order to do what is expressly authorized or required by the warrant;

(b) conduct for obtaining related communications data; and

(c) conduct by any person which is conduct in pursuance of a requirement imposed by or on behalf of the person to whom the warrant is addressed to be provided with assistance with giving effect to the warrant.

11 Application for and issue of interception warrant

(1) An interception warrant may be issued only on an application by or on behalf of –

(a) the Chief Officer;

(b) the Agent of the Impôts;

(c) the Chief Inspector of Immigration;

(d) the Director General of the Security Services;

(e) the Chief of the Secret Intelligence Services;

(f) the Director of GCHQ;

(g) the Chief of Defence Intelligence of the Ministry of Defence of the Government of the United Kingdom;

(h) a person who, for the purposes of any international mutual assistance agreement, is the competent authority of a country or territory outside Jersey.

(2) An interception warrant shall not be issued except under the hand of the Attorney General.

(3) An interception warrant must be addressed to the person falling within paragraph (1) by whom, or on whose behalf, the application for the warrant was made.

12 Contents of warrants

(1) An interception warrant must name or describe either –

(a) one person as the interception subject; or

(b) a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place.

(2) The provisions of an interception warrant describing communications the interception of which is authorized or required by the warrant must comprise one or more schedules setting out the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications that may be or are to be intercepted.

(3) Any factor or combination of factors set out in accordance with paragraph (2) must be one that identifies communications which are likely to be or to include –

(a) communications from, or intended for, the person named or described in the warrant in accordance with paragraph (1); or

(b) communications originating on, or intended for transmission to, the premises so named or described.

(4) Paragraphs (1) and (2) shall not apply to an interception warrant if –

(a) the description of communications to which the warrant relates confines the conduct authorized or required by the warrant to –

(i) the interception of communications sent or received outside Jersey in the course of their transmission by means of a telecommunication system, and

(ii) any conduct authorized in relation to any such interception by Article 10(6);

and

(b) at the time of the issue of the warrant, a certificate applicable to the warrant has been issued by and under the hand of the Attorney General certifying –

(i) the descriptions of intercepted material the examination of which the Attorney General considers necessary, and

(ii) that the Attorney General considers the examination of material of those descriptions necessary as mentioned in Article 10(3)(a), (b) or (c).

13 Duration, cancellation and renewal of warrants

(1) An interception warrant –

(a) shall cease to have effect at the end of the relevant period; but

(b) may be renewed, at any time before the end of that period, by an instrument under the hand of the Attorney General.

(2) The Attorney General –

(a) shall not renew an interception warrant under paragraph (1) unless he or she believes that the warrant continues to be necessary on grounds falling within Article 10(3); and

(b) shall cancel an interception warrant if satisfied that the warrant is no longer necessary on grounds falling within Article 10(3).

(3) In this Article "the relevant period" –

(a) in relation to a renewed warrant the latest renewal of which was by an instrument endorsed under the hand of the Attorney General with a statement that the renewal is believed to be

necessary on grounds falling within Article 10(3)(a) or (c), means the period of 6 months beginnin with the day of the warrant's renewal; and

(b) in any other case, means the period of 3 months beginning with the day of the warrant's issue or, in the case of a warrant that has been renewed, of its latest renewal.

14 Modification of warrants and certificates

(1) The Attorney General may at any time –

(a) modify the provisions of an interception warrant; or

(b) modify an Article 12(4) certificate so as to include in the certified material any material the examination of which the Attorney General considers to be necessary as mentioned in Article 10(3)(a), (b) or (c).

(2) If at any time the Attorney General considers that any factor set out in a schedule to an interception warrant is no longer relevant for identifying communications which, in the case of that warrant, are likely to be or to include communications falling within Article 12(3)(a) or (b), the Attorney General shall modify the warrant by the deletion of that factor.

(3) If at any time the Attorney General considers that the material certified by an Article 12(4) certificate includes any material the examination of which is no longer necessary as mentioned in any of paragraphs (a) to (c) of Article 10(3), the Attorney General shall modify the certificate so as t exclude that material from the certified material.

(4) Subject to paragraph (5), a warrant or certificate shall not be modified under this Article except by an instrument under the hand of the Attorney General.

(5) Where modifications in accordance with this paragraph are expressly authorized by provision contained in the warrant, the scheduled parts of an interception warrant may, in an urgent case, be modified by an instrument under the hand of –

(a) the person to whom the warrant is addressed; or

(b) a person holding any such position subordinate to that person as may be identified in the provisions of the warrant.

(6) For the purposes of this Article –

(a) the scheduled parts of an interception warrant are any provisions of the warrant that are contained in a schedule of identifying factors comprised in the warrant for the purposes of Article 12(2); and

(b) the modifications that are modifications of the scheduled parts of an interception warrant include the insertion of an additional such schedule in the warrant,

and references in this Article to unscheduled parts of an interception warrant, and to their modification, shall be construed accordingly.

15 Implementation of warrants

(1) Effect may be given to an interception warrant either –

(a) by the person to whom it is addressed; or

(b) by that person acting through, or together with, such other persons as he or she may require (whether under paragraph (2) or otherwise) to provide assistance with giving effect to the warrant.

(2) The person to whom an interception warrant is addressed may, for the purpose of requiring any person to provide assistance in relation to the warrant –

(a) serve a copy of the warrant on such persons as he or she considers may be able to provide such assistance; or

(b) make arrangements under which a copy of it is to be or may be so served.

(3) The copy of an interception warrant that is served on any person under paragraph (2) may, to the extent authorized –

(a) by the person to whom the warrant is addressed; or

(b) by the arrangements made by the person to whom the warrant is addressed for the purposes of that paragraph,

omit any one or more of the schedules to the warrant.

(4) Where a copy of an interception warrant has been served by or on behalf of the person to whom it is addressed on –

(a) a person who provides a postal service;

(b) a person who provides a public telecommunications service; or

(c) a person not falling within sub-paragraph (b) who has control of the whole or any part of a telecommunication system located wholly or partly in Jersey,

it shall (subject to paragraph (5)) be the duty of that person to take all such steps for giving effect to the warrant as are notified to him or her by or on behalf of the person to whom the warrant is addressed.

(5) A person who is under a duty by virtue of paragraph (4) to take steps for giving effect to a warrant shall not be required to take any steps which it is not reasonably practicable for that person to take.

(6) For the purposes of paragraph (5) the steps which it is reasonably practicable for a person to take in a case in which obligations have been imposed on that person by or under Article 16 shall include every step which it would have been reasonably practicable for that person to take had that person complied with all the obligations so imposed on him or her.

(7) A person who knowingly fails to comply with his or her duty under paragraph (4) shall be guilty of an offence and liable to imprisonment for a term not exceeding 2 years or to a fine, or both.

(8) A person's duty under paragraph (4) to take steps for giving effect to a warrant shall be enforceable by civil proceedings by the Attorney General for an injunction or for any other appropriate relief.

(9) For the purposes of this Law the provision of assistance with giving effect to an interception warrant includes any disclosure to the person to whom the warrant is addressed, or to persons acting on that person's behalf, of intercepted material obtained by any interception authorized or required by the warrant, and of any related communications data.

16 Maintenance of interception capability

(1) The Committee may by Order provide for the imposition by it on persons who –

(a) are providing public postal services or public telecommunications services; or

(b) are proposing to do so,

of such obligations as it appears to the Committee reasonable to impose for the purpose of securing that it is and remains practicable for requirements to provide assistance in relation to interception warrants to be imposed and complied with.

(2) The Committee's power to impose the obligations provided for by an Order under this Article shall be exercisable by the giving, in accordance with the Order, of a notice requiring the person who is to be subject to the obligations to take all such steps as may be specified or described in the notice.

(3) Subject to paragraph (10), the only steps that may be specified or described in a notice given to a person under paragraph (2) are steps appearing to the Committee to be necessary for securing that the person has the practical capability of providing any assistance which that person may be required to provide in relation to relevant interception warrants.

(4) A person shall not be liable to have an obligation imposed on him or her in accordance with an Order under this Article by reason only that the person provides, or is proposing to provide, to members of the public a telecommunications service the provision of which is or, as the case may be, will be no more than –

(a) the means by which that person provides a service which is not a telecommunications service; or

(b) necessarily incidental to the provision by that person of a service which is not a telecommunications service.

(5) A person to whom a notice is given under paragraph (2) otherwise than by virtue of paragraph (6)(c may refer the notice to the Technical Advisory Board.

(6) Where a person refers a notice given under paragraph (2) to the Technical Advisory Board–

(a) the person shall not be required to comply with any obligation imposed by the notice, unless the notice is given by virtue of sub-paragraph (c)(ii);

(b) the Board shall consider the technical requirements and the financial consequences, for the person making the reference, of the notice referred to them and shall report their conclusions on those matters to that person and to the Committee; and

(c) the Committee, after considering any report of the Board relating to the notice, may either –

(i) withdraw the notice, or

(ii) give a further notice under paragraph (2) confirming its effect, with or without modifications.

(7) It shall be the duty of a person to whom a notice is given under paragraph (2) to comply with the notice; and that duty shall be enforceable by civil proceedings by the Attorney General for an injunction or for any other appropriate relief.

(8) A notice for the purposes of paragraph (2) must specify such period as appears to the Committee to be reasonable as the period within which the steps specified or described in the notice are to be taken.

(9) Before making an Order under this Article the Committee shall consult with –

(a) such persons appearing to it to be likely to be subject to the obligations for which it provides;

(b) the Technical Advisory Board;

(c) such persons representing persons falling within sub-paragraph (a); and

(d) such persons with statutory functions in relation to persons falling within that sub-paragraph,

as the Committee considers appropriate.

(10) For the purposes of this Article the question whether a person has the practical capability of providing assistance in relation to relevant interception warrants shall include the question whether all such arrangements have been made as the Committee considers necessary –

(a) with respect to the disclosure of intercepted material;

(b) for the purpose of ensuring that security and confidentiality are maintained in relation to, and to matters connected with, the provision of any such assistance; and

(c) for the purpose of facilitating the carrying out of any functions in relation to this Chapter of the Commissioner,

but before determining for the purposes of the making of any Order, or the imposition of any obligation, under this Article what arrangements it considers necessary for the purpose mentioned in sub-paragraph (c) the Committee shall consult the Commissioner.

(11) In this Article "relevant interception warrant" –

(a) in relation to a person providing a public postal service, means an interception warrant relating to the interception of communications in the course of their transmission by means of that service; and

(b) in relation to a person providing a public telecommunications service, means an interception warrant relating to the interception of communications in the course of their transmission by means of a telecommunication system used for the purposes of that service.

17 Technical Advisory Board

(1) There shall be a Technical Advisory Board, whose members shall be appointed by the Committee.

(2) The Committee, in appointing the members of the Technical Advisory Board, shall ensure –

(a) that the membership of the Board includes persons likely effectively to represent the interests of the persons on whom obligations may be imposed under Article 16;

(b) that the membership of the Board includes persons likely effectively to represent the interests of the persons by or on whose behalf applications for interception warrants may be made; and

(c) that the Board is so constituted as to produce a balance between the representation of the interests mentioned respectively in sub-paragraphs (a) and (b).

(3) The Committee may, if the Committee thinks fit, appoint persons as members of the Technical Advisory Board in addition to those described in paragraph (2).

18 Grants for interception costs

(1) It shall be the duty of the States to ensure that such arrangements are in force as are necessary for securing that a person who provides –

(a) a postal service; or

(b) a telecommunications service,

receives such contribution as is, in the circumstances of that person's case, a fair contribution towards the costs incurred, or likely to be incurred, by that person in consequence of the matters mentioned in paragraph (2).

(2) Those matters are –

(a) in relation to a person providing a postal service, the issue of interception warrants relating to communications transmitted by means of that postal service;

(b) in relation to a person providing a telecommunications service, the issue of interception warrants relating to communications transmitted by means of a telecommunication system used for the purposes of that service;

(c) in relation to each description of person, the imposition on that person of obligations provided for by an Order under Article 16.

(3) Contributions made pursuant to this Article shall be paid out of the annual income of the States.

19 General safeguards for intercepted material

(1) Subject to paragraph (6), Attorney General shall ensure, in relation to all interception warrants, that such arrangements are in force as the Attorney General considers necessary for securing –

(a) that the requirements of paragraphs (2) and (3) are satisfied in relation to the intercepted material and any related communications data; and

(b) in the case of warrants in relation to which there are Article 12(4) certificates, that the requirements of Article 20 are also satisfied.

(2) The requirements of this paragraph are satisfied in relation to the intercepted material and any related communications data if each of the following matters is limited to the minimum that is necessary for the authorized purposes, namely –

(a) the number of persons to whom any of the material or data is disclosed or otherwise made

available;

(b) the extent to which any of the material or data is disclosed or otherwise made available;

(c) the extent to which any of the material or data is copied; and

(d) the number of copies that are made.

(3) The requirements of this paragraph are satisfied in relation to the intercepted material and any related communications data if each copy made of any of the material or data (if not destroyed earlier) is destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorized purposes.

(4) For the purposes of this Article something is necessary for the authorized purposes if, and only if –

(a) it continues to be, or is likely to become, necessary as mentioned in Article 10(3);

(b) it is necessary for facilitating the carrying out of any of the functions under this Chapter of the Attorney General;

(c) it is necessary for facilitating the carrying out of any functions in relation to this Part of the Commissioner or of the Tribunal; or

(d) it is necessary to ensure that a person conducting a criminal prosecution has the information needed to determine what is required of that person by his or her duty to secure the fairness of the prosecution.

(5) The arrangements for the time being in force under this Article for securing that the requirements of paragraph (2) are satisfied in relation to the intercepted material or any related communications data shall include such arrangements as the Attorney General considers necessary for securing that every copy of the material or data that is made is stored, for so long as it is retained, in a secure manner.

(6) Arrangements in relation to interception warrants which are made for the purposes of paragraph (1)–

(a) shall not be required to secure that the requirements of paragraphs (2) and (3) are satisfied in so far as they relate to any of the intercepted material or related communications data, or any copy of any such material or data, possession of which has been surrendered to any authorities of a country or territory outside Jersey; but

(b) shall be required to secure, in the case of every such warrant, that possession of the intercepted material and data and of copies of the material or data is surrendered to authorities of a country or territory outside Jersey only if it appears to the Attorney General –

(i) that requirements corresponding to those of paragraphs (2) and (3) will apply, to such extent (if any) as the Attorney General thinks fit, in relation to any of the intercepted material or related communications data possession of which, or of any copy of which, is surrendered to the authorities in question, and

(ii) that restrictions are in force which would prevent, to such extent (if any) as the Attorney General thinks fit, the doing of anything in, for the purposes of or in connection with any proceedings outside Jersey which would result in such a disclosure as, by virtue of Article 21, could not be made in Jersey.

(7) In this Article "copy", in relation to intercepted material or related communications data, means any of the following (whether or not in documentary form) –

(a) any copy, extract or summary of the material or data which identifies itself as the product of an interception; and

(b) any record referring to an interception which is a record of the identities of the persons to or by whom the intercepted material was sent, or to whom the communications data relates,

and "copied" shall be construed accordingly.

20 Extra safeguards for warrant with Article 12(4) certificate

(1) For the purposes of Article 19(1)(b) the requirements of this Article, in the case of a warrant in

relation to which there is an Article 12(4) certificate, are that the intercepted material is read, looked at or listened to by the persons to whom it becomes available by virtue of the warrant to the extent only that it –

(a) has been certified as material the examination of which is necessary as mentioned in Article 10(3)(a), (b) or (c); and

(b) falls within paragraph (2).

(2) Subject to paragraphs (3) and (4), intercepted material falls within this paragraph so far only as it is selected to be read, looked at or listened to otherwise than according to a factor which –

(a) is referable to an individual who is known to be for the time being in Jersey; and

(b) has as its purpose, or one of its purposes, the identification of material contained in communications sent by or intended for that individual.

(3) Intercepted material falls within paragraph (2), notwithstanding that it is selected by reference to any such factor as is mentioned in sub-paragraphs (a) and (b) of that paragraph, if–

(a) it is certified by the Attorney General for the purposes of Article 12(4) that the examination of material selected according to factors referable to the individual in question is necessary as mentioned in Article 10(3)(a), (b) or (c); and

(b) the material relates only to communications sent during a period of not more than 3 months specified in the certificate.

(4) Intercepted material also falls within paragraph (2), notwithstanding that it is selected by reference to any such factor as is mentioned in sub-paragraphs (a) and (b) of that paragraph, if–

(a) the person to whom the warrant is addressed believes, on reasonable grounds, that the circumstances are such that the material would fall within that paragraph; or

(b) the conditions set out in paragraph (5) are satisfied in relation to the selection of the material.

(5) Those conditions are satisfied in relation to the selection of intercepted material if –

(a) it has appeared to the person to whom the warrant is addressed that there has been such a relevant change of circumstances as, but for paragraph (4)(b), would prevent the intercepted material from falling within paragraph (2);

(b) since it first so appeared, a written authorization to read, look at or listen to the material has been given by the Attorney General; and

(c) the selection is made before the end of the first working day after the day on which it first so appeared to that person.

(6) References in this Article to its appearing that there has been a relevant change of circumstances are references to its appearing either –

(a) that the individual in question has entered Jersey; or

(b) that a belief by the person to whom the warrant is addressed in the individual's presence outside Jersey was in fact mistaken.

21 Exclusion of matters from legal proceedings

(1) Subject to Article 22, no evidence shall be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings which (in any manner) –

(a) discloses, in circumstances from which its origin in anything falling within paragraph (2) may be inferred, any of the contents of an intercepted communication or any related communications data; or

(b) tends (apart from any such disclosure) to suggest that anything falling within paragraph (2) has or may have occurred or be going to occur.

(2) The following fall within this paragraph –

(a) conduct by a person falling within paragraph (3) that would be or was an offence under Article 5(1) or (2) of this Law or under Article 2 of theInterception of Communications (Jersey) Law 1993[12];

(b) a breach by the Attorney General of the Attorney General's duty under Article 5(4) of this Law;

(c) the issue of an interception warrant or of a warrant under the Interception of Communications (Jersey) Law 1993[13];

(d) the making of an application by any person for an interception warrant, or for a warrant under that Law;

(e) the imposition of any requirement on any person to provide assistance with giving effect to an interception warrant.

(3) The persons referred to in paragraph (2)(a) are–

(a) any person to whom a warrant under this Chapter may be addressed;

(b) any person holding office in any administration of the States or of a Committee of the States;

(c) any person holding office or employed in the Law Officers Department;

(d) an officer of the Force or member of the Honorary Police;

(e) an immigration officer;

(f) any person employed by or for the purposes of the Force or the Honorary Police;

(g) any person providing a postal service or employed for the purposes of any business of providing such a service;

(h) any person providing a public telecommunications service or employed for the purposes of any business of providing such a service; and

(i) any member of the intelligence services.

(4) In this Article "intercepted communication" means any communication intercepted in the course of its transmission by means of a postal service or telecommunication system.

22 Exceptions to Article 21

(1) Article 21(1) shall not apply in relation to–

(a) any proceedings for a relevant offence;

(b) any civil proceedings under Article 15(8);

(c) any proceedings before the Tribunal;

(d) any proceedings on an appeal for which provision is made by an order under Article 56(8);

(e) any proceedings before the Proscribed Organizations Appeal Commission or any proceedings arising out of proceedings before that Commission.

(2) Paragraph (1) shall not, by virtue of sub-paragraph (e), authorize the disclosure of anything to–

(a) the applicant to the Proscribed Organizations Appeal Commission;

(b) the organization concerned (if different);

(c) any person designated under paragraph 6(2) of Schedule 2 to the Terrorism (Jersey) Law 2002[14] to conduct proceedings so falling on behalf of that organization; or

(d) any person who for the purposes of any proceedings so falling (but otherwise than by virtue of an appointment under paragraph 7 of that Schedule) represents that applicant or that organization.

(3) Article 21(1) shall not prohibit anything done in, for the purposes of, or in connection with, so much of any legal proceedings as relates to whether conduct constituting an offence under Article 5(1)

or (2), 15(7) or 23 of this Law, or Article 2 of the Interception of Communications (Jersey) Law 1993[15] constitutes a proper ground for dismissal.

(4) Article 21(1)(a) shall not prohibit the disclosure of any of the contents of a communication if the interception of that communication was lawful by virtue of Article 7(c), 8 or 9.

(5) Where any disclosure is proposed to be or has been made on the grounds that it is authorized by paragraph (4), Article 21(1) shall not prohibit the doing of anything in, or for the purposes of, so much of any legal proceedings as relates to the question whether that disclosure is or was so authorized.

(6) Article 21(1)(b) shall not prohibit the doing of anything that discloses any conduct of a person for which the person has been convicted of an offence under Article 5(1) or (2), 15(7) or 23 of this Law, or Article 2 of the Interception of Communications (Jersey) Law 1993[16]

(7) Nothing in Article 21(1) shall prohibit any such disclosure of any information that continues to be available for disclosure as is confined to –

(a) a disclosure to a person conducting a criminal prosecution for the purpose only of enabling that person to determine what is required of that person by his or her duty to secure the fairness of the prosecution; or

(b) a disclosure to the Bailiff in a case in which the Bailiff has ordered the disclosure to be made to the Bailiff alone.

(8) The Bailiff shall not order a disclosure under paragraph (7)(b) except where the Bailiff is satisfied that the exceptional circumstances of the case make the disclosure essential in the interests of justice.

(9) Subject to paragraph (10), where in any criminal proceedings–

(a) the Bailiff orders a disclosure under paragraph (7)(b); and

(b) in consequence of that disclosure the Bailiff is of the opinion that there are exceptional circumstances requiring him or her to do so,

the Bailiff may direct the person conducting the prosecution to make, for the purposes of the proceedings, any such admission of fact as the Bailiff thinks essential in the interests of justice.

(10) Nothing in any direction under paragraph (9) shall authorize or require anything to be done in contravention of Article 21(1).

(11) In this Article "relevant offence" means –

(a) an offence under any provision of this Law;

(b) an offence under Article 2 of the Interception of Communications (Jersey) Law 1993;[17]

(c) an offence under section 5 of the 1949 Act;

(d) an offence under Article 34 of the Post Office (Jersey) Law 1969[18] or under Article 52 of the Telecommunications (Jersey) Law 2002;[19]

(e) an offence under Article 3 or 4 of the Official Secrets (Jersey) Law 1952[20] relating to any sketch, plan, model, article, note, document or information which incorporates or relates to the contents of any intercepted communication or any related communications data or tends to suggest as mentioned in Article 17(1)(b) of this Law;

(f) perjury committed in the course of any proceedings mentioned in paragraph (1) or (3) of this Article;

(g) attempting or conspiring to commit, or aiding, abetting, counselling or procuring the commission of, an offence falling within any of the preceding sub-paragraphs; and

(h) contempt of court committed in the course of, or in relation to, any proceedings mentioned in paragraph (1) or (3) of this Article.

(12) In paragraph (11)"intercepted communication" has the same meaning as in Article 21.

23 Offence for unauthorized disclosures

(1) Where an interception warrant has been issued or renewed, it shall be the duty of every person falling within paragraph (2) to keep secret all the matters mentioned in paragraph (3).

(2) The persons falling within this paragraph are –

(a) the persons specified in Article 11(1);

(b) every person holding office in an administration of the States or of a Committee of the States;

(c) every person holding office or employed in the Law Officers Department;

(d) every officer of the Force or member of the Honorary Police;

(e) every immigration officer;

(f) every person employed by or for the purposes of the Force or the Honorary Police;

(g) persons providing postal services or employed for the purposes of any business of providing such a service;

(h) persons providing public telecommunications services or employed for the purposes of any business of providing such a service;

(i) persons having control of the whole or any part of a telecommunication system located wholly or partly in Jersey;

(j) every member of the intelligence services;

(k) every official of the Ministry of Defence of the Government of the United Kingdom.

(3) The matters to be kept secret are –

(a) the existence and contents of the warrant and of any Article 12(4) certificate in relation to the warrant;

(b) the details of the issue of the warrant and of any renewal or modification of the warrant or of any such certificate;

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

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

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

(4) A person who makes a disclosure to another person of anything that the firstmentioned person is required to keep secret under this Article shall be 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 shall be a defence for the accused to show that the accused could not reasonably have been expected, after first becoming aware of the matter disclosed, to take steps to prevent the disclosure.

(6) In proceedings against any person for an offence under this Article in respect of any disclosure, it shall be 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.

(7) In proceedings against any person for an offence under this Article in respect of any disclosure, it shall be 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 t furthering any criminal purpose.

(9) In proceedings against any person for an offence under this Article in respect of any disclosure, it shall be 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 warrant or the person to whom the warrant is or was addressed;

(c) by the terms of the requirement to provide assistance; or

(d) by Article 15(9).

CHAPTER 2

ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

24 Interpretation of Chapter 2

In this Chapter –

"communications data" means any of the following –

(a) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;

(b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person–

(i) of any postal service or telecommunications service, or

(ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;

(c) any information not falling within paragraph (a) or (b) that is held or obtained, in relation tc persons to whom he or she provides the service, by a person providing a postal service or telecommunications service;

"designated" shall be construed in accordance with Article 29(1);

"postal or telecommunications operator" means a person who provides a postal service or telecommunications service;

"relevant public authority" shall be construed in accordance with Article 29(1).

25 Lawful acquisition and disclosure of communications data

(1) This Chapter applies to –

(a) any conduct in relation to a postal service or telecommunication system for obtaining communications data, other than conduct consisting in the interception of communications in the course of their transmission by means of such a service or system; and

(b) the disclosure to any person of communications data.

(2) Conduct to which this Chapter applies shall be lawful for all purposes if –

(a) it is conduct in which any person is authorized or required to engage by an authorization or

notice granted or given under this Chapter; and

(b) the conduct is in accordance with, or in pursuance of, the authorization or requirement.

(3) A person shall not be subject to any civil liability in respect of any conduct of that person which –

(a) is incidental to any conduct that is lawful by virtue of paragraph (2); and

(b) is not itself conduct for which an authorization or warrant –

(i) is capable of being granted under this Law, section 5 of the 1994 Act or Article 101 o the Police Procedures and Criminal Evidence (Jersey) Law 2003[21] and

(ii) might reasonably have been expected to have been sought in the case in question.

26 Authorizations and notices to obtain and disclose communications data

(1) This Article applies where a person designated for the purposes of this Chapter believes that it is necessary on grounds falling within paragraph (2) to obtain any communications data.

(2) It is necessary on grounds falling within this paragraph to obtain communications data if it is necessary –

(a) in the interests of national security;

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

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

(d) in the interests of public safety;

(e) for the purpose of protecting public health;

(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to any administration of the States or of a Committee of the States;

(g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or

(h) for any purpose (not falling within sub-paragraphs (a) to (g)) which is specified for the purposes of this paragraph by Regulations made by the States.

(3) Subject to paragraph (5), a designated person may grant an authorization for persons holding offices ranks or positions with the relevant public authority in relation to which that person is designated to engage in any conduct to which this Chapter applies.

(4) Subject to paragraph (5), where it appears to the designated person that a postal o telecommunications operator is or may be in possession of, or be capable of obtaining, any communications data, the designated person may, by notice to the postal or telecommunications operator, require the operator –

(a) if the operator is not already in possession of the data, to obtain the data; and

(b) in any case, to disclose all of the data in the operator's possession or subsequently obtained by the operator.

(5) The designated person shall not grant an authorization under paragraph (3), or give a notice under paragraph (4), unless that person believes that obtaining the data in question by the conduc authorized or required by the authorization or notice is proportionate to what is sought to be achieved by so obtaining the data.

(6) It shall be the duty of the postal or telecommunications operator to comply with the requirements of any notice given to the operator under paragraph (4).

(7) A person who is under a duty by virtue of paragraph (6) shall not be required to do anything in pursuance of that duty which it is not reasonably practicable for that person to do.

(8) The duty imposed by paragraph (6) shall be enforceable by civil proceedings by the Attorney Genera

for an injunction, or for any other appropriate relief.

27 Form and duration of authorizations and notices

(1) An authorization under Article 26(3)–

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

(b) shall describe the conduct to which this Chapter applies that is authorized and the communications data in relation to which it is authorized;

(c) shall specify the grounds in Article 26(2) on which it is necessary to obtain the data; and

(d) shall specify the office, rank or position held by the person granting the authorization.

(2) A notice under Article 26(4) requiring communications data to be disclosed or to be obtained and disclosed –

(a) shall 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) shall describe the communications data to be obtained or disclosed under the notice;

(c) shall specify the grounds in Article 26(2) on which it is necessary to obtain the data;

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

(e) shall specify the manner in which any disclosure required by the notice is to be made.

(3) A notice under Article 26(4) shall not require the disclosure of data to any person other than–

(a) the designated 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,

but the provisions of a notice given by a designated person other than the Attorney General shall not specify or otherwise identify a person for the purposes of sub-paragraph (b) unless the person holds an office, rank or position with the same relevant public authority as the designated person.

(4) An authorization under Article 26(3) or notice under Article 26(4)–

(a) shall not authorize or require any data to be obtained after the end of the period of one month beginning with the date on which the authorization is granted or the notice given; and

(b) in the case of a notice, shall not authorize or require any disclosure after the end of that period of any data not in the possession of, or obtained by, the postal or telecommunications operator at a time during that period.

(5) An authorization under Article 26(3) or notice under Article 26(4) may be renewed at any time before the end of the period of one month applying (in accordance with paragraph (4) or paragraph (7)) to that authorization or notice.

(6) A renewal of an authorization under Article 26(3) or of a notice under Article 26(4) shall be by the grant or giving, in accordance with this Article, of a further authorization or notice.

(7) Paragraph (4) shall have effect in relation to a renewed authorization or renewal notice as if the period of one month mentioned in that paragraph did not begin until the end of the period of one month applicable to the authorization or notice that is current at the time of the renewal.

(8) A person who has given a notice under Article 26(4) shall cancel the notice if satisfied–

(a) that it is no longer necessary on grounds falling within paragraph (2) of that Article for the requirements of the notice to be complied with; or

(b) that the conduct required by the notice is no longer proportionate to what is sought to be achieved by obtaining communications data to which the notice relates.

(9) The Committee may by Order provide for the person by whom any duty imposed by paragraph (8) is

to be performed in a case in which it would otherwise fall on a person who is no longer available to perform it; and an Order under this paragraph may provide for the person on whom the duty is to fall to be a person appointed in accordance with the Order.

28 Arrangements for payments

(1) The States shall ensure that such arrangements are in force as they think appropriate for requiring or authorizing, in such cases as they think fit, the making to postal and telecommunications operators of appropriate contributions towards the costs incurred by them in complying with notices under Article 26(4).

(2) Any contributions under this Article shall be paid out of the annual income of the States.

29 Persons designated to give authorizations and notices under this Chapter

(1) Schedule 1 shall have effect to designate persons for the purposes of this Chapter and specify the public authorities in relation to which they are designated.

(2) The States may by Regulations –

(a) amend Schedule 1 so as to –

(i) remove a public authority and the person designated in relation to that authority,

(i) subject to paragraphs (2) and (3), add a public authority and designate a person ir relation to that authority,

(iii) subject to paragraph (4), change the designated person in relation to a public authority;

(b) impose restrictions –

(i) on the authorizations and notices under this Chapter that may be granted or given by any individual holding an office, rank or position with a specified public authority, and

(ii) on the circumstances in which, or the purposes for which, such authorizations may be granted or notices given by any such individual.

(3) The States may only amend Schedule 1 so as to add a public authority outside Jersey if the authority is –

(a) a police force of a country or territory outside the British Islands and Northern Ireland;

(b) a public authority in the British Islands or Northern Ireland having functions which consist of or include the provision of criminal intelligence, the prevention and detection of serious crime, the investigation of crimes and the charging of offences;

(c) a public authority of a country or territory outside the British Islands and Northern Ireland whose functions correspond to those of a police force or otherwise consist of or include the investigation of conduct contrary to the law of that country or territory, or the apprehension of persons guilty of such conduct;

(d) a public authority with functions under any international agreement which consist of or include –

(i) the investigation of conduct which is unlawful under the law of one or more places, prohibited by such an agreement or contrary to international law, or

(ii) the apprehension of persons guilty of such conduct.

(4) Only the Attorney General may be the designated person in relation to any of the intelligence services, the Ministry of Defence of the Government of the United Kingdom or Her Majesty's Forces or any other public authority outside Jersey added to Schedule 1 pursuant to paragraph (3).

PART 3

30 Interpretation of Part 3

(1) In this Part –

"private vehicle" means (subject to paragraph (3)(a)) any vehicle which is used primarily for the private purposes of the person who owns it or of a person otherwise having the right to use it;

"residential premises" means (subject to paragraph (3)(b)) so much of any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation (including hotel or prison accommodation that is so occupied or used);

"surveillance device" means any apparatus designed or adapted for use in surveillance.

(2) References in this Part to an individual holding an office or position with a public authority include references to any member, official or employee of that authority.

(3) In paragraph (1)–

(a) the reference to a person having the right to use a vehicle does not, in relation to a motor vehicle, include a reference to a person whose right to use the vehicle derives only from that person having paid, or undertaken to pay, for the use of the vehicle and its driver for a particular journey; and

(b) the reference to premises occupied or used by any person for residential purposes or otherwise as living accommodation does not include a reference to so much of any premises as constitutes any common area to which that person has or is allowed access in connection with his or her use or occupation of any accommodation.

(4) In this Article –

"premises" includes any vehicle or moveable structure and any other place whatever, whether or not occupied as land;

"vehicle" includes any vessel, aircraft or hovercraft.

31 Meaning of "surveillance"

(1) Subject to paragraph (2), in this Part"surveillance" includes –

(a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;

(b) recording anything monitored, observed or listened to in the course of surveillance; and

(c) surveillance by or with the assistance of a surveillance device.

(2) References in this Part to surveillance do not include references to –

(a) any conduct of a covert human intelligence source for obtaining or recording (whether or not using a surveillance device) any information which is disclosed in the presence of the source;

(b) the use of a covert human intelligence source for so obtaining or recording information; or

(c) any such entry on or interference with property or with wireless telegraphy as would be unlawful unless authorized under –

(i) section 5 of the 1994 Act, or

(ii) Article 101 of thePolice Procedures and Criminal Evidence (Jersey) Law 2003[22]

(3) References in this Part to surveillance include references to the interception of a communication in the course of its transmission by means of a postal service or telecommunication system if, and only if –

(a) the communication is one sent by or intended for a person who has consented to the

interception of communications sent by or to that person; and

(b) there is no interception warrant authorizing the interception.

32 Meaning of "directed surveillance", "intrusive surveillance" and "covert human intelligence source"

(1) Subject to paragraph (5), surveillance is directed for the purposes of this Part if it is covert but not intrusive and is undertaken –

(a) for the purposes of a specific investigation or a specific operation;

(b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and

(c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorization under this Part to be sought for the carrying out of the surveillance.

(2) Subject to paragraphs (3) to (5), surveillance is intrusive for the purposes of this Part if, and only if, it is covert surveillance that –

(a) is carried out in relation to anything taking place on any residential premises or in any private vehicle; and

(b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

(3) For the purposes of this Part surveillance is not intrusive to the extent that –

(a) it is carried out by means only of a surveillance device designed or adapted principally for the purpose of providing information about the location of a vehicle; or

(b) it is surveillance consisting in any such interception of a communication as falls within Article 31(3).

(4) For the purposes of this Part surveillance which –

(a) is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle; but

(b) is carried out without that device being present on the premises or in the vehicle,

is not intrusive unless the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

(5) For the purposes of this Part surveillance which –

(a) is carried out by means of apparatus designed or adapted for the purpose of detecting the installation or use in any residential or other premises of a television receiver (within the meaning of section 1 of the 1949 Act); and

(b) is carried out from outside those premises exclusively for that purpose,

is neither directed nor intrusive.

(6) In this Part –

(a) references to the conduct of a covert human intelligence source are references to any conduct of such a source which falls within any of sub-paragraphs (a) to (c) of paragraph (7), or is incidental to anything falling within any of those paragraphs; and

(b) references to the use of a covert human intelligence source are references to inducing, asking or assisting a person to engage in the conduct of such a source, or to obtain information by means of the conduct of such a source.

(7) For the purposes of this Part a person is a covert human intelligence source if –

(a) he or she establishes or maintains a personal or other relationship with a person for the covert

purpose of facilitating the doing of anything falling within sub-paragraph (b) or (c);

(b) he or she covertly uses such a relationship to obtain information or to provide access to any information to another person; or

(c) he or she covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

(8) For the purposes of this Part the activities of a covert human intelligence source which are to be taken as activities for the benefit of a particular public authority include any conduct of that person as such a source which is in response to inducements or requests made by or on behalf of that authority.

(9) For the purposes of this Article –

(a) surveillance is covert if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place;

(b) a purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose; and

(c) a relationship is used covertly, and information obtained as mentioned in paragraph (7)(c) is disclosed covertly, if and only if it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

(10) In this Article "private information", in relation to a person, includes any information relating to that person's private or family life.

(11) References in this Article, in relation to a vehicle, to the presence of a surveillance device in the vehicle include references to its being located on or under the vehicle and also include references to its being attached to it.

33 Lawful surveillance etc.

(1) This Part applies to the following conduct –

(a) directed surveillance;

(b) intrusive surveillance; and

(c) the conduct and use of covert human intelligence sources.

(2) Conduct to which this Part applies shall be lawful for all purposes if –

(a) an authorization under this Part confers an entitlement to engage in that conduct on the person whose conduct it is; and

(b) that person's conduct is in accordance with the authorization.

(3) A person shall not be subject to any civil liability in respect of any conduct of that person which –

(a) is incidental to any conduct that is lawful by virtue of paragraph (2); and

(b) is not itself conduct an authorization or warrant for which –

(i) is capable of being granted under this Law, section 5 of the 1994 Act or Article 101 of the Police Procedures and Criminal Evidence (Jersey) Law 2003[23] and

(ii) might reasonably have been expected to have been sought in the case in question.

(4) The conduct that may be authorized under this Part includes conduct outside Jersey.

34 Authorization of directed surveillance

(1) Subject to the following provisions of this Part, the persons designated for the purposes of this Article shall each have power to grant authorizations for the carrying out of directed surveillance.

(2) A person shall not grant an authorization for the carrying out of directed surveillance unless the person believes –

(a) that the authorization is necessary on grounds falling within paragraph (3); and

(b) that the authorized surveillance is proportionate to what is sought to be achieved by carrying it out.

(3) An authorization 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 of preventing disorder;

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

(d) in the interests of public safety;

(e) for the purpose of protecting public health;

(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to any administration of the States or of a Committee of the States; or

(g) for any purpose (not falling within sub-paragraphs (a) to (f)) which is prescribed.

(4) The conduct that is authorized by an authorization for the carrying out of directed surveillance is any conduct that –

(a) consists in the carrying out of directed surveillance of any such description as is specified in the authorization; and

(b) is carried out in the circumstances described in the authorization and for the purposes of the investigation or operation specified or described in the authorization.

35 Authorization of covert human intelligence sources

(1) Subject to the following provisions of this Part, the persons designated for the purposes of this Article shall each have power to grant authorizations for the conduct or the use of a covert human intelligence source.

(2) A person shall not grant an authorization for the conduct or the use of a covert human intelligence source unless the person believes –

(a) that the authorization is necessary on grounds falling within paragraph (3);

(b) that the authorized conduct or use is proportionate to what is sought to be achieved by that conduct or use; and

(c) that arrangements exist for the source's case that satisfy the requirements of paragraph (5) and such other requirements as may be prescribed.

(3) An authorization 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 of preventing disorder;

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

(d) in the interests of public safety;

(e) for the purpose of protecting public health;

(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable any administration of the States or of a Committee of the States; or

(g) for any purpose (not falling within sub-paragraphs (a) to (f)) which is prescribed.

(4) The conduct that is authorized by an authorization for the conduct or the use of a covert human intelligence source is any conduct that –

(a) is comprised in any such activities involving conduct of a covert human intelligence source, or

the use of a covert human intelligence source, as are specified or described in the authorization;

(b) consists in conduct by or in relation to the person who is so specified or described as the person to whose actions as a covert human intelligence source the authorization relates; and

(c) is carried out for the purposes of, or in connection with, the investigation or operation so specified or described.

(5) For the purposes of this Part there are arrangements for the source's case that satisfy the requirements of this paragraph if such arrangements are in force as are necessary for ensuring –

(a) that there will at all times be a person holding an office, rank or position with the relevant investigating authority who will have day-to-day responsibility for dealing with the source on behalf of that authority, and for the source's security and welfare;

(b) that there will at all times be another person holding an office, rank or position with the relevant investigating authority who will have general oversight of the use made of the source;

(c) that there will at all times be a person holding an office, rank or position with the relevant investigating authority who will have responsibility for maintaining a record of the use made of the source;

(d) that the records relating to the source that are maintained by the relevant investigating authority will always contain particulars of all such matters (if any) as may be prescribed; and

(e) that records maintained by the relevant investigating authority that disclose the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available to those persons.

(6) The Committee may by Order –

(a) prohibit the authorization under this Article of any such conduct or uses of covert human intelligence sources as may be described in the Order; and

(b) impose requirements, in addition to those provided for by paragraph (2), that must be satisfied before an authorization is granted under this Article for any such conduct or uses of covert human intelligence sources as may be so described.

(7) In this Article "relevant investigating authority", in relation to an authorization for the conduct or the use of an individual as a covert human intelligence source, means (subject to paragraph (8)) the public authority for whose benefit the activities of that individual as such a source are to take place.

(8) In the case of any authorization for the conduct or the use of a covert human intelligence source whose activities are to be for the benefit of more than one public authority, the references in paragraph (5) to the relevant investigating authority are references to one of them (whether or not the same one in the case of each reference).

36 Designated persons and public authorities for Articles 34 and 35

(1) Part 1 of Schedule 2 shall have effect to specify public authorities and the persons designated in relation to them for the purposes of Articles 34 and 35.

(2) Part 2 of Schedule 2 shall have effect to specify public authorities and the persons designated in relation to them for the purposes of Article 34 only.

(3) The States may by Regulations –

(a) subject to paragraph (4), amend Schedule 2 so as to–

(i) remove a public authority and the person designated in relation to that authority,

(ii) add a public authority and designate a person in relation to that authority,

(iii) change the person designated in relation to a public authority;

(b) impose restrictions –

(i) on the authorizations under Articles 34 and 35 that may be granted by any individual designated in relation to a specified public authority, and

(ii) on the circumstances in which, or the purposes for which, such authorizations may be granted by any such individual.

(4) Only the Attorney General may be the designated person in relation to any of the intelligence services, the Ministry of Defence of the Government of the United Kingdom or Her Majesty's Forces.

37 Authorization of intrusive surveillance

(1) Subject to the following provisions of this Part, the Attorney General may grant authorizations for the carrying out of intrusive surveillance on the application of –

(a) the Chief Officer;

(b) the Agent of the Impôts;

(c) the Chief Inspector of Immigration;

(d) any member of the intelligence services;

(e) any official of the Ministry of Defence of the Government of the United Kingdom; or

(f) a member of Her Majesty's Forces.

(2) The Attorney General shall not grant an authorization for the carrying out of intrusive surveillance unless the Attorney General believes –

(a) that the authorization is necessary on grounds falling within paragraph (3); and

(b) that the authorized surveillance is proportionate to what is sought to be achieved by carrying it out.

(3) Subject to paragraphs (4) to (6), an authorization 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 serious crime; or

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

(4) The Attorney General shall not grant an authorization on the ground described in paragraph (3)(c) on the application of any person mentioned in paragraph (1)(d), (e) or (f).

(5) The matters to be taken into account in considering whether the requirements of paragraph (2) are satisfied in the case of any authorization shall include whether the information which it is thought necessary to obtain by the authorized conduct could reasonably be obtained by other means.

(6) The conduct that is authorized by an authorization for the carrying out of intrusive surveillance is any conduct that –

(a) consists in the carrying out of intrusive surveillance of any such description as is specified in the authorization;

(b) is carried out in relation to the residential premises specified or described in the authorization or in relation to the private vehicle so specified or described; and

(c) is carried out for the purposes of, or in connection with, the investigation or operation so specified or described.

(7) Where an Order has been made under section 41(4) of the Regulation of Investigatory Powers Act 2000 of the United Kingdom Parliament limiting the individuals who may apply under subsection (1) of that section to individuals of an office, rank or position prescribed in that Order, an application may be made under paragraph (1)(d), (e) or (f) only by an individual of the office, rank or position so prescribed.

(8) References in this Article to a member of Her Majesty's Forces do not include references to any member of Her Majesty's Forces who is a member of a police force by virtue of his or her service with the Royal Navy Regulating Branch, the Royal Military Police or the Royal Air Force Police.

38 Rules for grant of authorizations

(1) A person, other than the Attorney General, who is a designated person for the purposes of Article 34 or 35 in respect of a specified public authority shall not grant an authorization under that Article except on an application made by a member of the same authority.

(2) A single authorization by the Attorney General may combine an authorization under this Part and an authorization under Article 101 of the Police Procedures and Criminal Evidence (Jersey) Law 2003 [24]

39 Notification of authorizations for intrusive surveillance

(1) The Attorney General shall from time to time and, in any event, at least every 12 months, notify the Commissioner, in writing, of authorizations for the carrying out of intrusive surveillance given, renewed or cancelled by the Attorney General and, where an authorization was given orally, of the grounds on which the case was believed to be urgent.

(2) Paragraph (1) is without prejudice to the Commissioner's general power to require the disclosure or provision of documents and information under Article 52.

40 General rules for grant, renewal and duration of authorizations

(1) An authorization under this Part –

(a) may be granted or renewed orally in any urgent case; and

(b) in any other case, must be in writing.

(2) A single authorization may combine 2 or more different authorizations under this Part; but the provisions of this Law that are applicable in the case of each of the authorizations shall apply separately in relation to the part of the combined authorization to which they are applicable.

(3) Subject to paragraphs (4) and (8), an authorization under this Part shall cease to have effect at the end of the following period –

(a) in the case of an authorization which –

(i) has not been renewed and was granted orally or by a person whose entitlement to act is confined to urgent cases, or

(ii) was last renewed orally,

the period of 72 hours beginning with the time when the grant of the authorization or, as the case may be, its latest renewal takes effect;

(b) in a case not falling within sub-paragraph (a) in which the authorization is for the conduct or the use of a covert human intelligence source, the period of 12 months beginning with the day on which the grant of the authorization or, as the case may be, its latest renewal takes effect; and

(c) in any case not falling within sub-paragraph (a) or (b), the period of 3 months beginning with the day on which the grant of the authorization or, as the case may be, its latest renewal takes effect.

(4) Subject to paragraph (6), an authorization under this Part may be renewed, at any time before the time at which it ceases to have effect, by the person who would be entitled to grant a new authorization in the same terms.

(5) Articles 34 to 39 shall have effect in relation to the renewal of an authorization under this Part as if references to the grant of an authorization included references to its renewal.

(6) A person shall not renew an authorization for the conduct or the use of a covert human intelligence

source, unless the person –

(a) is satisfied that a review has been carried out of the matters mentioned in paragraph (7); and

(b) has, for the purpose of deciding whether he or she should renew the authorization, considered the results of that review.

(7) The matters mentioned in paragraph (6) are–

(a) the use made of the source in the period since the grant or, as the case may be, latest renewal of the authorization; and

(b) the tasks given to the source during that period and the information obtained from the conduct or the use of the source.

(8) The Committee may by Order provide in relation to authorizations of such descriptions as may be specified in the Order that paragraph (3) is to have effect as if the period at the end of which ar authorization of a description so specified is to cease to have effect were such period shorter than that provided for by that paragraph as may be fixed by or determined in accordance with that Order.

(9) References in this Article to the time at which, or the day on which, the grant or renewal of an authorization takes effect are references –

(a) in the case of the grant of an authorization, to the time at which or, as the case may be, day on which the authorization is granted;

(b) in the case of the renewal of an authorization, to the time at which or, as the case may be, day on which the authorization would have ceased to have effect but for the renewal.

41 Cancellation of authorizations

(1) The person who granted or, as the case may be, last renewed an authorization under this Part shall cancel it if –

(a) that person is satisfied that the authorization is one in relation to which the requirements of Article 34(2), 35(2) or 37(2), as the case may be, are no longer satisfied; or

(b) in the case of an authorization under Article 35, that person is satisfied that arrangements for the source's case that satisfy the requirements mentioned in paragraph (2)(c) of that Article no longer exist.

(2) Where an authorization under this Part was granted or, as the case may be, last renewed –

(a) by a person entitled to act for any other person; or

(b) by the deputy of any other person,

that other person shall cancel the authorization if he or she is satisfied as to either of the matters mentioned in paragraph (1).

(3) Where an authorization under this Part was granted or, as the case may be, last renewed by a person whose deputy had power to grant it, that deputy shall cancel the authorization if he or she is satisfied as to either of the matters mentioned in paragraph (1).

(4) The Committee may by Order provide for the person by whom any duty imposed by this Article is to be performed in a case in which it would otherwise fall on a person who is no longer available to perform it.

(5) An Order under paragraph (4) may provide for the person on whom the duty is to fall to be a person appointed in accordance with the Order.

42 Power to extend or modify authorization provisions

The States may by Regulations do one or both of the following –

(a) apply this Part, with such modifications as they think fit, to any such surveillance that is neither

directed nor intrusive as may be described in the Regulations;

(b) provide for any description of directed surveillance to be treated for the purposes of this Part as intrusive surveillance.

PART 4

INVESTIGATION OF ELECTRONIC DATA PROTECTED BY ENCRYPTION ETC.

43 Interpretation of Part 4

(1) In this Part –

"electronic signature" means anything in electronic form which –

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

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

(c) is 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 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;

"police" means the Force;

"protected information" means any electronic data which, 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 44 notice" means a notice under Article 44;

"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 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 something's being intelligible or being put into an intelligible form include references to its being in the condition in which it was before an encryption or similar process was applied to it or, as the case may be, to its 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.

44 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 police, the Customs and Excise or the Immigration and Nationality Department or is likely so to come into the possession of any of those services, the police, the Customs and Excise or the Immigration and Nationality Department.

(2) If any person with the appropriate permission under Schedule 3 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 3 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 shall 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 shall 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) shall 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 shall 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 shall not require the disclosure of any key which –

(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.

(11) Schedule 3 shall have effect.

45 Effect of notice imposing disclosure requirement

(1) Subject to the following provisions of this Article, the effect of an Article 44 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) shall be 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) shall be required, in accordance with the notice imposing the requirement, to make a disclosure of the information in an intelligible form.

(2) A person subject to a requirement under paragraph (1)(b) to make a disclosure of any information in an intelligible form shall be 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, in a case in which a disclosure requirement in respect of any protected information is imposed on any person by an Article 44 notice–

(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 46, 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 that he or she shall be required, 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 44 notice; and

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

(5) It shall not be 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 shall not 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 44 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 have 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 that that person shall be required, in accordance with the notice imposing the requirement, 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 that 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 44 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.

46 Cases in which key required

(1) An Article 44 notice imposing a disclosure requirement in respect of any protected information shall not contain a statement for the purposes of Article 45(3)(c) unless–

(a) the person who for the purposes of Schedule 3 granted the permission for the giving of the notice in relation to that information; or

(b) any person whose permission for the giving of a such a notice in relation to that information would constitute the appropriate permission under 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 police, Customs and Excise or the Immigration and Nationality Department shall not be given –

(a) in the case of a direction by the police, except by or with the permission of the Chief Officer;

(b) in the case of a direction by the Customs and Excise, except by or with the permission of the Agent of the Impôts; or

(c) in the case of a direction by the Immigration and Nationality Department, except by or with the permission of the Chief Inspector of Immigration.

(3) A permission given for the purposes of paragraph (2) must be given expressly in relation to the direction in question.

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

(a) that there are special circumstances of the case which 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.

(5) The matters to be taken into account in considering whether the requirement of paragraph (4)(b) is satisfied in the case of any direction shall 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.

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

(7) A notification under paragraph (6)–

(a) must be given not more 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.

47 Contribution to costs of disclosure

(1) It shall be the duty of the States to ensure that such arrangements are in force as they think appropriate for requiring or authorizing, in such cases as they think fit, the making to persons to whom Article 44 notices are given of appropriate contributions towards the costs incurred by them in complying with such notices.

(2) Contributions made pursuant to this Article shall be paid out of the annual income of the States.

48 Offence: failure to comply with a notice

(1) It shall be an offence for a person to whom an Article 44 notice has been given to knowingly fail, in accordance with the notice, to make the disclosure required by virtue of the giving of 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 44 notice, the accused shall be 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 shall be 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 44 notice before 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 shall be liable to imprisonment for a term of 2 years and to a fine.

49 Offence: tipping-off

(1) This Article applies where an Article 44 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 shall not be included in an Article 44 notice except where–

(a) it is included with the consent of the person who for the purposes of Schedule 3 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 have constituted appropriate permission under that Schedule.

(3) An Article 44 notice shall 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 police, Customs and Excise, the Immigration and Nationality Department or any of the intelligence services; or

(b) is likely to come into the possession of the police, Customs and Excise, the Immigration and Nationality Department or any of the intelligence services,

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 44 notice to keep secret shall be 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 shall be 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 shall be 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 shall be 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 shall be 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 44(1).

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

50 General duties of specified authorities

(1) This Article applies to –

(a) the Attorney General;

(b) every Committee of the States;

(c) the Chief Officer;

(d) the Agent of the Impôts;

(e) the Chief Inspector of Immigration; and

(f) every other person whose officers or employees include persons with duties that involve the giving of Article 44 notices.

(2) It shall be the duty of each of the persons to whom this Article applies to ensure that such arrangements are in force, 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 44 notice is used for obtaining access to, or putting into an intelligible form, only protected information in relation to which 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 44 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 44 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 in pursuance of that paragraph in relation to persons under the control of a person to whom this Article applies,

the breach or contravention shall be 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 44 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 shall have regard to any opinion with respect to the matters to which the proceedings relate that is or has been given by the Commissioner.

PART 5

SCRUTINY ETC. OF INVESTIGATORY POWERS

51 Investigatory Powers Commissioner

(1) The Bailiff shall appoint one of the ordinary judges of the Court of Appeal who is not the President of the Tribunal as the Investigatory Powers Commissioner to carry out the function described in this Article.

(2) Subject to paragraph (4), the Commissioner shall keep under review–

(a) the exercise and performance by the Attorney General of the powers and duties conferred or imposed on the Attorney General by or under Articles 5 to 15;

(b) the exercise and performance, by the persons on whom they are conferred or imposed, of the powers and duties conferred or imposed by or under Chapter 2 of Part 2;

(c) the exercise and performance, by the person on whom they are conferred or imposed, of the powers and duties conferred or imposed by or under Part 3;

(d) 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 4;

(e) the adequacy of the arrangements by virtue of which the duty which is imposed on the Attorney General by Article 19 are sought to be discharged;

(f) the adequacy of the arrangements by virtue of which the duties imposed by Article 50 are sought to be discharged in relation to persons whose conduct is under review under sub-paragraph (b).

(3) The Commissioner shall give the Tribunal all such assistance (including the Commissioner's opinion as to any issue falling to be determined by the Tribunal) as the Tribunal may require –

(a) in connection with the investigation of any matter by the Tribunal; or

(b) otherwise for the purposes of the Tribunal's consideration or determination of any matter.

(4) The Commissioner shall hold office in accordance with the terms of his or her appointment; and there shall be paid to the Commissioner out of money provided by the States such allowances as the Finance and Economics Committee may direct.

(5) The Committee, after consultation with the Finance and Economics Committee and the Commissioner, shall –

(a) make such technical facilities available to the Commissioner, and

(b) provide the Commissioner with such staff,

as are sufficient to secure that the Commissioner is able properly to carry out his or her functions.

(6) On the coming into force of this Article the person holding office as Commissioner under Article 9 of the Interception of Communications (Jersey) Law 1993[25] shall take and hold office as Commissioner as if appointed under this Law –

(a) for the unexpired period of that person's term of office under the first mentioned Law; and

(b) otherwise, on the terms of that person's appointment under the first mentioned Law.

52 Co-operation with and reports by the Commissioner

(1) It shall be the duty of –

(a) every person holding office or employed in any administration of the States or of a Committee of the States;

(b) every person holding office in Jersey under the Crown;

(c) every person holding office or employed in the Law Officers Department;

(d) every officer of the Force and member of the Honorary Police;

(e) every member of each of the intelligence services;

(f) every official of the Ministry of Defence of the Government of the United Kingdom;

(g) every member of Her Majesty's Forces;

(h) every person employed by or for the purposes of the Force or the honorary police;

(i) every person required for the purposes of Article 15 to provide assistance with giving effect to an interception warrant;

(j) every person on whom an obligation to take any steps has been imposed under Article 16;

(k) every person by or to whom an authorization under Article 26(3) has been granted;

(l) every person to whom a notice under Article 26(4) has been given;

(m) every person by or to whom an authorization under Article 34, 35 or 37 has been granted;

(n) every person to whom a notice under Article 44 has been given in relation to any information obtained under Part 2; and

(o) every person who is or has been employed for the purposes of any business of a person falling within sub-paragraph (i), (j), (l) or (n),

to disclose or provide to the Commissioner all such documents and information as the Commissioner may require in order to carry out the Commissioner's functions under Article 51.

(2) If it at any time appears to the Commissioner –

(a) that there has been a contravention of the provisions of this Law in relation to any matter with which the Commissioner is concerned; and

(b) that the contravention has not been the subject of a report made to the Bailiff by the Tribunal,

the Commissioner shall make a report to the Bailiff with respect to that contravention.

(3) If it at any time it appears to the Commissioner that any arrangements by reference to which the duties imposed by Articles 19 and 50 have sought to be discharged have proved inadequate in relation to any matter with which the Commissioner is concerned, the Commissioner shall make a report to the Bailiff with respect to those arrangements.

(4) As soon as practicable after the end of each calendar year, the Commissioner shall make a report to the Bailiff with respect to the carrying out of the Commissioner's functions.

(5) The Commissioner may also, at any time, make any such other report to the Bailiff on any matter relating to the carrying out of the Commissioner's functions as the Commissioner thinks fit.

(6) The Bailiff shall cause a copy of every annual report made by the Commissioner under paragraph (4) to be laid before the States, together with a statement as to whether any matter has been excluded from that copy in pursuant to paragraph (7).

(7) If it appears to the Bailiff, after consultation with the Commissioner, that the publication of any matter in an annual report would be contrary to the public interest or prejudicial to –

(a) national security;

(b) the prevention or detection of serious crime;

(c) the economic well-being of Jersey; or

(d) the continued discharge of the functions of any public authority whose activities include activities that are subject to review by the Commissioner,

the Bailiff may exclude that matter from the copy of the report as laid before the States.

53 Assistant Investigatory Powers Commissioners

(1) The Bailiff may, after consultation with the Commissioner as to numbers, appoint as Assistant Investigatory Powers Commissioners such number of persons as the Bailiff considers necessary for the purpose of providing the Commissioner with assistance under this Article.

(2) A person shall not be appointed as an Assistant Commissioner unless the person holds or has held office as –

(a) a judge of the Royal Court;

(b) a judge of the Crown Court in England;

(c) a sheriff in Scotland;

(d) a county court judge or resident magistrate in Northern Ireland;

(e) a judge of the Royal Court of Guernsey; or

(f) a judge of the High Court of the Isle of Man.

(3) The Commissioner may –

(a) require any Assistant Commissioner to provide assistance in carrying out the Commissioner's functions under Article 51(2); and

(b) delegate any of those functions to an Assistant Commissioner, subject to such conditions and restrictions, if any, as the Commissioner thinks fit.

(4) The assistance that may be provided under this Article includes –

(a) the conduct on behalf of the Commissioner of the review of any matter; and

(b) the making of a report to the Commissioner about the matter reviewed.

(5) An Assistant Commissioner shall be subject to the duty imposed on the Commissioner by Article 51(3).

(6) An Assistant Commissioner shall hold office in accordance with the terms of his or her appointment, and there shall be paid to an Assistant Commissioner out of money provided by the States such

allowances as the Finance and Economics Committee may direct.

54 Investigatory Powers Tribunal

(1) There shall be an Investigatory Powers Tribunal which shall consist of 3 members appointed by the Superior Number of the Royal Court of whom one shall be an ordinary judge of the Court of Appeal, who shall be the president of the Tribunal, and 2 shall be Jurats.

(2) Notwithstanding Article 8(1)(a) of the Human Rights (Jersey) Law 2000[26] proceedings falling with paragraph (4) of this Article which are brought pursuant to the said Article 8 shall be brought befor the Tribunal.

(3) The jurisdiction of the Tribunal shall be –

(a) to consider and determine any complaints made to them which, in accordance with paragraph (5), are complaints for which the Tribunal is the appropriate forum;

(b) to consider and determine any reference to them by any person that the person has suffered detriment as a consequence of any prohibition or restriction, by virtue of Article 21, on tha person's relying in, or for the purposes of, any civil proceedings on any matter; and

(c) to hear and determine any other such proceedings falling within paragraph (4) as may be allocated to them in accordance with provision made by the Committee by Order.

(4) Proceedings fall within this paragraph if –

(a) they are proceedings against any of the intelligence services in respect of any discharge of their functions within Jersey;

(b) they are proceedings against any other person in respect of any conduct, or proposed conduct, by or on behalf of any of those services in the discharge of such functions;

(c) they are proceedings brought by virtue of Article 50(4); or

(d) they are proceedings relating to the taking place in any challengeable circumstances of any conduct falling within paragraph (6).

(5) The Tribunal shall be the appropriate forum for any complaint if it is a complaint by a person who is aggrieved by any conduct falling within paragraph (6) which the person believes–

(a) to have taken place in relation to that person, to any of that person's property, to any communications sent by or to that person, or intended for that person, or to that person's use of any postal service, telecommunications service or telecommunication system; and

(b) to have taken place in challengeable circumstances or to have been carried out by or on behalf of any of the intelligence services.

(6) Subject to paragraph (7), conduct falls within this paragraph if (whenever it occurred) it is–

(a) conduct by or on behalf of any of the intelligence services;

(b) conduct for or in connection with the interception of communications in the course of their transmission by means of a postal service or telecommunication system;

(c) conduct to which Chapter 2 of Part 2 applies;

(d) conduct to which Part 3 applies;

(e) the giving of a notice under Article 44 or any disclosure or use of a key to protected information;

(f) any entry on or interference with property or any interference with wireless telegraphy.

(7) For the purposes only of paragraph (4), nothing mentioned in paragraph (d) or (f) of paragraph (6) shall be treated as falling within that paragraph unless it is conduct by or on behalf of a person holding any office, rank or position with or employed by –

(a) any of the intelligence services;

(b) any of Her Majesty's Forces;

(c) the Force or the Honorary Police;

(d) Customs and Excise;

(e) the Immigration and Nationality Department.

(8) For the purposes of this Article conduct takes place in challengeable circumstances if –

(a) it takes place with the authority, or purported authority, of anything falling within paragraph (9); or

(b) the circumstances are such that (whether or not there is such authority) it would not have been appropriate for the conduct to take place without it, or at least without proper consideration having been given to whether such authority should be sought,

but conduct does not take place in challengeable circumstances to the extent that it is authorized by, or takes place with the permission of, the Bailiff.

(9) The following fall within this paragraph –

(a) an interception warrant;

(b) an authorization or notice under Chapter 2 of Part 2;

(c) an authorization under Part 3;

(d) a permission for the purposes of Schedule 3;

(e) a notice under Article 44;

(f) an authorization under Article 101 of the Police Procedures and Criminal Evidence (Jersey) Law 2003[27] or

(g) a warrant under the Interception of Communications (Jersey) Law 1993[28]

(10) Schedule 4 shall have effect to make further provision regarding the members of the Tribunal and appointment of officers.

(11) In this Article –

(a) references to a key and to protected information shall be construed in accordance with Article 43(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 43(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 43(2).

55 Orders allocating proceedings to the Tribunal

(1) An Order under Article 54(3)(c) allocating proceedings to the Tribunal–

(a) may provide for the Tribunal to exercise jurisdiction in relation to that matter to the exclusion of the jurisdiction of any court or tribunal; but

(b) if it does so provide, must contain provision conferring a power on the Tribunal, in the circumstances provided for in the Order, to remit the proceedings to the court or tribunal which would have had jurisdiction apart from the Order.

(2) In making any provision by an Order under Article 54(3)(c) the Committee shall have regard, in particular, to –

(a) the need to secure that proceedings allocated to the Tribunal are properly heard and considered;

and

(b) the need to secure that information is not disclosed to an extent, or in a manner, that is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic well-being of Jersey or the continued discharge, within Jersey, of the functions of any of the intelligence services.

56 Exercise of the Tribunal's jurisdiction

(1) Subject to paragraphs (4) and (5), it shall be the duty of the Tribunal–

(a) to hear and determine any proceedings brought before them by virtue of Article 54(3)(c); and

(b) to consider and determine any complaint or reference made to them by virtue of Article 54(3)(a) or (b).

(2) Where the Tribunal hear any proceedings by virtue of Article 54(2), they shall apply the same principles for making their determination in those proceedings as would be applied by a court on an application for judicial review.

(3) Where the Tribunal consider a complaint made to them by virtue of Article 54(3)(a), it shall be the duty of the Tribunal –

(a) to investigate whether the persons against whom any allegations are made in the complaint have engaged, in relation to –

(i) the complainant,

(ii) any of the complainant's property,

(iii) any communications sent by or to the complainant, or intended for the complainant, or

(iv) the complainant's use of any postal service, telecommunications service or telecommunication system,

in any conduct falling within Article 54(6);

(b) to investigate the authority (if any) for any conduct falling within Article 54(6) which they find has been so engaged in; and

(c) in relation to the Tribunal's findings from their investigations, to determine the complaint by applying the same principles as would be applied by a court on an application for judicial review.

(4) The Tribunal shall not be under any duty to hear, consider or determine any proceedings, complaint or reference if it appears to them that the bringing of the proceedings or the making of the complaint or reference is frivolous or vexatious.

(5) Except where the Tribunal, having regard to all the circumstances, are satisfied that it is equitable to do so, they shall not consider or determine any complaint made by virtue of Article 54(3)(a) if it is made more than one year after the taking place of the conduct to which it relates.

(6) Subject to rules made under Article 58, where any proceedings have been brought before the Tribunal or any reference made to the Tribunal, they shall have power to make such interim orders, pending their final determination, as they think fit.

(7) Subject to any provision made by rules under Article 58, the Tribunal on determining any proceedings, complaint or reference shall have power to make any such award of compensation or other order as they think fit; and, without prejudice to the power to make rules under Article 58(2)(g), the other orders that may be made by the Tribunal include –

(a) an order quashing or cancelling any warrant or authorization; and

(b) an order requiring the destruction of any records of information which –

(i) has been obtained in exercise of any power conferred by a warrant or authorization, or

(ii) is held by any public authority in relation to any person.

(8) The Committee –

(a) shall, by Order, make provision allowing for an appeal to the Royal Court against any exercise by the Tribunal of their jurisdiction under Article 54(3)(b) or (c); and

(b) may, by Order, make provision for an appeal against any other determination, award, order or other decision of the Tribunal,

but a determination, order, award or other decision of the Tribunal, including a decision as to whether they have jurisdiction, shall not otherwise be subject to appeal or be liable to be questioned in any court.

57 Tribunal procedure

(1) Subject to rules made under Article 58, the Tribunal shall be entitled to determine their owr procedure in relation to any proceedings, complaint or reference brought before or made to them.

(2) The Tribunal shall have power –

(a) in connection with the investigation of any matter; or

(b) otherwise for the purposes of the Tribunal's consideration or determination of any matter,

to require the Commissioner to provide the Tribunal with all such assistance (including the Commissioner's opinion as to any issue falling to be determined by the Tribunal) as the Tribunal think fit.

(3) Where the Tribunal hear or consider any proceedings, complaint or reference relating to any matter, they shall secure that the Commissioner –

(a) is aware that the matter is the subject of proceedings, a complaint or a reference brought before or made to the Tribunal; and

(b) is kept informed of any determination, award, order or other decision made by the Tribunal with respect to that matter.

(4) Where the Tribunal determine any proceedings, complaint or reference brought before or made to them, they shall give notice to the complainant which (subject to any rules made by virtue of Article 58(2)(h) may be confined, as the case may be, to either–

(a) a statement that they have made a determination in the complainant's favour; or

(b) a statement that no determination has been made in the complainant's favour.

(5) Where –

(a) the Tribunal make a determination in favour of any person by whom any proceedings have been brought before the Tribunal or by whom any complaint or reference has been made to the Tribunal; and

(b) the determination relates to any act or omission by or on behalf of the Attorney General or to conduct for which any warrant, authorization or permission was issued, granted or given by the Attorney General,

they shall make a report of their findings to the Bailiff.

(6) It shall be the duty of the persons specified in paragraph (7) to disclose or provide to the Tribunal al such documents and information as the Tribunal may require for the purpose of enabling them –

(a) to exercise the jurisdiction conferred on them by or under Article 54; or

(b) otherwise to exercise or perform any power or duty conferred or imposed on them by or under this Law.

(7) Those persons are –

(a) every person holding office or employed in any administration of the States or of a Committee of the States;

(b) every person employed in Jersey under the Crown;

(c) every person holding office or employed in the Law Officers Department;

(d) every officer of the Force or member of the Honorary Police;

(e) every member of each of the intelligence services;

(f) every official of the Ministry of Defence of the Government of the United Kingdom;

(g) every person employed by or for the purposes of the Force or the Honorary Police;

(h) every person required for the purposes of Article 15 to provide assistance with giving effect to an interception warrant;

(i) every person on whom an obligation to take any steps has been imposed under Article 16;

(j) every person by or to whom an authorization under Article 26(3) has been granted;

(k) every person to whom a notice under Article 26(4) has been given;

(l) every person by whom, or on whose application, there has been granted or given any authorization under Part 3 of this Law or under Article 101 of the Police Procedures and Criminal Evidence (Jersey) Law 2003;[29]

(m) every person who holds or has held any office, rank or position with the same public authority as a person falling within sub-paragraph (l);

(n) every person who has engaged in any conduct with the authority of an authorization under Article 26 or Part 3 of this Law or under Article 101 of the Police Procedures and Criminal Evidence (Jersey) Law 2003;[30]

(o) every person who holds or has held any office, rank or position with a public authority for whose benefit any such authorization has been or may be given;

(p) every person to whom a notice under Article 44 has been given; and

(q) every person who is or has been employed for the purposes of any business of a person falling within paragraph (h), (i), (k) or (p).

(8) In this Article, a reference to the Commissioner includes a reference to any Assistant Commissioner who, under Article 53, assisted the Commissioner in the matter or to whom the Commissioner delegated any function in respect of the matter.

58 Tribunal rules

(1) The Bailiff may make rules regulating –

(a) the exercise by the Tribunal of the jurisdiction conferred on them by or under Article 54; and

(b) any matters preliminary or incidental to, or arising out of, the hearing or consideration of any proceedings, complaint or reference brought before or made to the Tribunal.

(2) Without prejudice to the generality of paragraph (1), rules under this Article may–

(a) enable different members of the Tribunal to carry out functions in relation to different complaints at the same time;

(b) specify the form and manner in which proceedings are to be brought before the Tribunal or a complaint or reference is to be made to the Tribunal;

(c) require persons bringing proceedings or making complaints or references to take such preliminary steps, and to make such disclosures, as may be specified in the rules for the purpose of facilitating a determination of whether –

(i) the bringing of the proceedings, or

(ii) the making of the complaint or reference,

is frivolous or vexatious;

(d) make provision about the determination of any question as to whether a person by whom –

(i) any proceedings have been brought before the Tribunal, or

(ii) any complaint or reference has been made to the Tribunal,

is a person with a right to bring those proceedings or make that complaint or reference;

(e) specify the forms of hearing or consideration to be adopted by the Tribunal in relation to particular proceedings, complaints or references (including a form that requires any proceedings brought before the Tribunal to be disposed of as if they were a complaint or reference made to the Tribunal);

(f) specify the practice and procedure to be followed on, or in connection with, the hearing or consideration of any proceedings, complaint or reference (including, where applicable, the mode and burden of proof and the admissibility of evidence);

(g) specify orders that may be made by the Tribunal under Article 56(6) or (7);

(h) require information about any determination, award, order or other decision made by the Tribunal in relation to any proceedings, complaint or reference to be provided (in addition to any statement under Article 57(4)) to the person who brought the proceedings or made the complaint or reference, or to the person representing his or her interests.

(3) Rules under this Article in relation to the hearing or consideration of any matter by the Tribunal may provide –

(a) for a person who has brought any proceedings before or made any complaint or reference to the Tribunal to have the right to be legally represented;

(b) for the manner in which the interests of a person who has brought any proceedings before or made any complaint or reference to the Tribunal may be represented;

(c) for the appointment in accordance with the rules, by such person as may be determined in accordance with the rules, of a person to represent those interests in the case of any proceedings, complaint or reference.

(4) The power to make rules under this Article includes power to make rules –

(a) enabling or requiring the Tribunal to hear or consider any proceedings, complaint or reference without the person who brought the proceedings or made the complaint or reference having been given full particulars of the reasons for any conduct which is the subject of the proceedings, complaint or reference;

(b) enabling or requiring the Tribunal to take any steps in exercise of their jurisdiction in the absence of any person (including the person bringing the proceedings or making the complaint or reference and any legal representative of that person);

(c) enabling or requiring the Tribunal, where evidence is taken in the absence of the person by whom the proceedings were brought or, as the case may be, the person who made the complaint or reference, to give that person a summary of the evidence so taken;

(d) enabling or requiring the Tribunal to exercise their jurisdiction, and to exercise and perform the powers and duties conferred or imposed on them (including, in particular, in relation to the giving of reasons), in such manner provided for in the rules as prevents or limits the disclosure of particular matters.

(5) Rules under this Article may also include provision –

(a) enabling powers or duties of the Tribunal that relate to matters preliminary or incidental to the hearing or consideration of any proceedings, complaint or reference to be exercised or performed by a single member of the Tribunal; and

(b) conferring on the Tribunal such ancillary powers as the Bailiff thinks necessary for the purposes of, or in connection with, the exercise of the Tribunal's jurisdiction, or the exercise or performance of any power or duty conferred or imposed on them.

(6) In making rules under this Article the Bailiff shall have regard, in particular, to –

(a) the need to secure that matters which are the subject of proceedings, complaints or references

brought before or made to the Tribunal are properly heard and considered; and

(b) the need to secure that information is not disclosed to an extent, or in a manner, that is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic well-being of Jersey or the discharge, within Jersey, of any functions of any of the intelligence services.

(7) Rules under this Article may make provision by the application, with or without modification, of the provision from time to time contained in specified rules of court.

59 Codes of practice

(1) The Committee may, in accordance with this Article, bring into operation one or more codes of practice relating to the exercise and performance of the powers and duties mentioned in paragraph (2).

(2) Those powers and duties are –

(a) those that are conferred or imposed (otherwise than on the Commissioner) by or under Parts 2 to 4 of this Law;

(b) those that are conferred or imposed (otherwise than on the Commissioner appointed under Article 104 of the Police Procedures and Criminal Evidence (Jersey) Law 2003[31]) by or under Part 11 of that Law.

(3) When the Committee proposes to bring into operation a code of practice, it shall prepare and publish a draft of that code, shall consider any representations made to it about the draft and may modify the draft accordingly.

(4) After the Committee has complied with paragraph (3), it may bring the code into operation by Order.

(5) An Order bringing a code of practice into operation may contain such transitional provisions and savings as appear to the Committee to be necessary or expedient in connection with the code of practice thereby brought into operation.

(6) The Committee may from time to time revise the whole or any part of a code of practice and bring into operation that revised code and paragraphs (3) to (5) shall apply, with appropriate modifications in relation to that revised code as they apply to the first code brought into operation.

60 Effect of codes of practice

(1) A person exercising or performing any power or duty in relation to which provision may be made by a code of practice under Article 59 shall, in doing so, have regard to the provisions (so far as they are applicable) of every code of practice for the time being in force under that Article.

(2) A failure on the part of any person to comply with any provision of a code of practice for the time being in force under Article 59 shall not of itself render that person liable to any criminal or civil proceedings.

(3) A code of practice in force at any time under Article 59 shall be admissible in evidence in any criminal or civil proceedings.

(4) If any provision of a code of practice issued or revised under Article 59 appears to–

(a) the court or tribunal conducting any civil or criminal proceedings;

(b) the Tribunal;

(c) the person carrying out the Commissioner's functions under this Law; or

(d) a person carrying out any functions of an Assistant Commissioner under Article 53 of this Law,

to be relevant to any question arising in the proceedings, or in connection with the exercise of that jurisdiction or the carrying out of those functions, in relation to a time when it was in force, that

provision of the code shall be taken into account in determining that question.

PART 6

SUPPLEMENTAL

61 Powers of delegation

(1) The Attorney General may delegate to a Crown Advocate any power conferred on the Attorney General by this Law as a person designated to grant an authorization or give a notice under Article 26 or grant an authorization under Article 34 or 35.

(2) The Committee may by Order –

(a) authorize the Chief Officer, the Agent of the Impôts or the Chief Inspector of Immigration to delegate all or any of the powers conferred on that person by this Law as a person designated to grant an authorization or give a notice under Article 26 or grant an authorization under Article 34 or 35 to an officer in the public authority in relation to which that person is designated of a rank or seniority specified in the Order; and

(b) impose any such conditions as it thinks fit upon the exercise of any power of delegation so conferred.

62 Expenditure

There shall be paid out of money provided by the States –

(a) any expenditure incurred by the Attorney General for or in connection with the carrying out of the Attorney General's functions under this Law; and

(b) any expenditure incurred by the Committee for or in connection with the carrying out of its functions under this Law;

(c) any increase attributable to this Law in the sums which are payable out of money so provided under any other enactment.

63 Power to prescribe by Order

The Committee may by Order prescribe anything that shall or may be prescribed under this Law.

64 Offences by body corporate, etc.

(1) Where an offence committed by a limited liability partnership or body corporate under this Law, other than an offence under any provision of Part 4, is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of –

(a) a person who is a partner of the partnership, or director, manager, secretary or other similar officer of the body corporate; or

(b) any person purporting to act in any such capacity,

the person shall also be guilty of the offence and liable in the same manner as the partnership or body corporate to the penalty provided for the offence.

(2) Where the affairs of a body corporate are managed by its members, paragraph (1) shall apply in relation to acts and defaults of a member in connection with the member's functions of management as if the member were a director of the body corporate.

65 General saving for lawful conduct

Nothing in any of the provisions of this Law by virtue of which conduct of any description is or may be authorized by any warrant, authorization or notice, or by virtue of which information may be obtained in any manner, shall be construed –

(a) as making it unlawful to engage in any conduct of that description which is not otherwise unlawful under this Law and would not be unlawful apart from this Law;

(b) as otherwise requiring –

(i) the issue, grant or giving of such a warrant, authorization or notice, or

(ii) the taking of any step for or towards obtaining the authority of such a warrant, authorization or notice,

before any such conduct of that description is engaged in; or

(c) as prejudicing any power to obtain information by any means not involving conduct that may be authorized under this Law.

66 Amendments, repeals, savings and transitional arrangements

(1) The enactments specified in Schedule 5 shall have effect with the amendments set out in that Schedule.

(2) The Interception of Communications (Jersey) Law 1993[32] is repealed.

(3) For the avoidance of doubt it is hereby declared that nothing in this Law (except paragraph 2 of Schedule 5) affects any power conferred on the Post Office by or under any enactment to open, detain or delay any postal packet or to deliver any such packet to a person other than the person to whom it is addressed.

(4) Where any warrant under the Interception of Communications (Jersey) Law 1993[33] is in force under that Law at the time when the repeal by this Law of Article 3 of that Law comes into force, the conduct authorized by that warrant shall be deemed for the period which –

(a) begins with that time; and

(b) ends with the time when that warrant would (without being renewed) have ceased to have effect under that Law,

as if it were conduct authorized by an interception warrant issued in accordance with the requirements of Chapter 1 of Part 2 of this Law.

(5) In relation to any such warrant, any certificate issued for the purposes of Article 4(2) of the Interception of Communications (Jersey) Law 1993[34] shall have effect in relation to that period as if it were a certificate issued for the purposes of Article 12(4) of this Law.

(6) Articles 19 and 20 of this Law shall have effect as if references to interception warrants and to Article 12(4) certificates included references, respectively, to warrants under Article 3 of the Interception of Communications (Jersey) Law 1993[35] and to certificates under Article 4(2) of that Law; and references in Articles 19 and 20 of this Law to intercepted or certified material shall be construed accordingly.

67 Citation and commencement

This Law may be cited as the Regulation of Investigatory Powers Act (Jersey) Law 200- and shall come into force on such day or days as the States by Act appoint and different days may be appointed for

different provisions of this Law and for different purposes.

SCHEDULE 1

(Article 29)

RELEVANT PUBLIC AUTHORITIES AND DESIGNATED PERSONS: COMMUNICATIONS DATA

Relevant public authority	*Designated person*
The Force	Chief Officer
Customs and Excise	Agent of the Impôts
Immigration and Nationality Department	Chief Inspector of Immigration
Income Tax Department	Attorney General
Any of the Parishes	Attorney General
Any of the intelligence services	Attorney General

SCHEDULE 2

(Article 36)

PUBLIC AUTHORITIES AND DESIGNATED PERSONS: SURVEILLANCE

PART 1

(Article 36(1))

PUBLIC AUTHORITIES AND DESIGNATED PERSONS: DIRECTED SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCES

Public authority	*Designated person*
The Force	Chief Officer
Customs and Excise	Agent of the Impôts
Immigration and Nationality Department	Chief Inspector of Immigration
Any of the intelligence services	Attorney General
Ministry of Defence of the Government of the United Kingdom	Attorney General
Income Tax Department	Attorney General
Agriculture and Fisheries Department	Attorney General
Environment and Public Services Department	Attorney General
Housing Department	Attorney General
Employment and Social Security Department	Attorney General
Health and Social Services Department	Attorney General
Jersey Financial Services Commission	Attorney General
Jersey Competition Regulatory Authority	Attorney General
Post Office	Attorney General
Any of the Parishes	Attorney General

PART 2

(Article 36(2))

PUBLIC AUTHORITIES AND DESIGNATED PERSONS: DIRECTED SURVEILLANCE ONLY

Public authority *Designated person*

SCHEDULE 3

(Article 44(11))

PERSONS HAVING THE APPROPRIATE PERMISSION

1 Interpretation

In this Schedule "authorization to interfere with property" means an authorization given under Article 101 of the Police Procedures and Criminal Evidence (Jersey) Law 2003.[36]

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 44 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 44(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 44 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,

shall be 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 of any Committee of the States, the Force, Customs and Excise and the Immigration and Nationality Department shall be 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, Customs and Excise and the Immigration and Nationality Department shall be 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 "the 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,

shall not 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 44(1)(a), (b) or (c) which is not information in the case of which paragraph 3 applies; and

(b) in the case of protected information falling within Article 44(1)(d) which is not information also falling within section 44(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 police, Customs and Excise or the Immigration and Nationality Department; or

(b) the information was provided or disclosed, or is likely to be provided or disclosed, to the police, Customs and Excise or the Immigration and Nationality Department; or

(c) the information is in the possession of, or is likely to come into the possession of, the police, Customs and Excise or the Immigration and Nationality Department,

the police, Customs and Excise or the Immigration and Nationality Department 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 shall 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 is of or above the rank of inspector; or

(b) permission to give an Article 44 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 police's possession by means of the exercise of powers conferred by Article 40 of the Terrorism (Jersey) Law 2002[37] 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 shall not entitle any person to give an Article 44 notice at any time after the permission has ceased to have effect.

(2) Such a permission, once granted, shall continue to have effect (notwithstanding 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

A permission for the purposes of any provision of this Schedule shall not be granted by the Attorney General except under the Attorney General's hand.

SCHEDULE 4

(Article 54(10))

THE TRIBUNAL

1 Membership of tribunal

(1) A member of the Tribunal shall vacate office at the end of the period of 5 years beginning with the day of the member's appointment, but shall be eligible for reappointment.

(2) A member of the Tribunal may be relieved of office by the Royal Court at the member's own request.

2 Salaries and expenses

There shall be paid to the members and officers of the Tribunal from money provided by the States such remuneration, allowances and expenses as the Finance and Economics Committee determine.

3 Officers

(1) The Finance and Economics Committee may, after consultation with the Tribunal, provide the Tribunal with such officers as it thinks necessary for the proper discharge of the Tribunal's functions.

(2) The Tribunal may authorize any officer provided under this paragraph to obtain any documents or information on the Tribunal's behalf.

SCHEDULE 5

(Article 66(1))

AMENDMENTS

1 Official Secrets (Jersey) Law 1952 amended

Article 12 of the Official Secrets (Jersey) Law 1952[38] shall be repealed.

2 Post Office (Jersey) Law 1969 amended

In the Post Office (Jersey) Law 1969 at the end of the proviso to Article 34[39] there shall be added the words "or under the authority of an interception warrant under Article 10 of the Regulation of Investigatory Powers (Jersey) Law 200-[40]".

3 Telecommunications (Jersey) Law 2002 amended

In the Telecommunications (Jersey) Law 2002–

(a) for Article 52(2) to (5)[41] there shall be substituted the following paragraph –

"(2) Paragraph (1) shall not apply to any disclosure made –

(a) in accordance with the order of any court or for the purposes of any criminal proceedings;

(b) in accordance with any warrant, authorization or notice issued, granted or given under any provision of the Regulation of Investigatory Powers (Jersey) Law 200-; [42]

(c) in compliance with any requirement imposed (apart from that Law) in consequence of the exercise by any person of any power conferred by or under any enactment exercisable by that person for the purpose of obtaining any document or other information; or

(d) in pursuance of any duty under the Regulation of Investigatory Powers (Jersey) Law 200-[43] or under Part 11 of the Police Procedures and Criminal Evidence (Jersey) Law 2003[44] to provide information or produce any document to the Investigatory Powers Commissioner appointed or the Investigatory Powers Commissioner established under the Regulation of Investigatory Powers (Jersey) Law 200-.[45]";

(b) in Schedule 1,[46] the amendments and repeals specified in relation to the Interception of Communications (Jersey) Law 1993[47] shall be deleted.

4 Terrorism (Jersey) Law 2002 amended

In Schedule 2 to the Terrorism (Jersey) Law 2002–

(a) in paragraphs 6(3) and 7(4),[48] for the words "In paragraphs (5) and (8)," there shall be substituted the words "In paragraph 5,";

(b) paragraph 8[49] shall be repealed.

5 Police Procedures and Criminal Evidence (Jersey) Law 2003 amended

(1) In this paragraph, the "Law" means the Police Procedures and Criminal Evidence (Jersey) Law 2003 [50]

(2) In Article 101 of the Law[51] –

(a) in paragraph (1), after the words "Attorney General" there shall be inserted the words ", on an application made by a person mentioned in paragraph (1A),";

(b) after paragraph (1) there shall be inserted the following paragraph–

"(1A) An application for an authorization under this Part may only be made by –

(a) the Chief Officer;

(b) the Agent of the Impôts;

(c) the Chief Inspector of Immigration;

(d) any member of the intelligence services;

(e) any official of the Ministry of Defence of the Government of the United Kingdom; or

(f) a member of Her Majesty's Forces.";

(c) for paragraph (4) there shall be substituted the following paragraphs–

"(4) The Committee may by Order –

(a) authorize the Chief Officer, the Agent of the Impôts or the Chief Inspector of Immigration to delegate the power, under paragraph (1A), to make an application under this Article to, respectively, a member of the Force, an officer of the Impôts or an immigration officer of a rank or seniority specified in the Order; and

(b) impose any such conditions as it thinks fit upon the exercise of any power of delegation so conferred.

(5) In this Article –

'Chief Inspector of Immigration' and 'immigration officer' have the same meaning as the Regulation of Investigatory Powers (Jersey) Law 200-[52];

'intelligence services' has the same meaning as in the Regulation of Investigatory Powers (Jersey) Law 200[53]

'serious crime' means conduct which constitutes one or more offences –

(a) which involves the use of violence, results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose; or

(b) for which a person who has attained the age of 21 and has no previous convictions could reasonably be expected to be sentenced to imprisonment for 3 years or more,

and references to a member of Her Majesty's Forces do not include references to any member of Her Majesty's Forces who is a member of a police force by virtue of his or her service with the Royal Navy Regulating Branch, the Royal Military Police or the Royal Air Force Police.".

(3) In Article 104 of the Law[54] –

(a) in paragraph (5), for the words "the security of the British Islands or to the detection of crime"

there shall be substituted the words "any of the purposes for which authorizations may be given or granted under this Part of this Law or Part 3 of the Regulation of Investigatory Powers (Jersey) Law 200[55]"; and

(b) after paragraph (5) there shall be added the following paragraph–

"(6) The Commissioner shall give the Investigatory Powers Tribunal established under Article 54(1) of the Regulation of Investigatory Powers (Jersey) Law 200[56] all such assistance (including the Commissioner's opinion as to any issue falling to be determined by that Tribunal) as that Tribunal may require –

(a) in connection with the investigation of any matter by that Tribunal; or

(b) otherwise for the purposes of that Tribunal's consideration or determination of any matter.".

[1] *Tome VIII, page 165, Volume 1990-1991, pages 389 and 844 and Volume 1996-1997, page 587.*

[2] *Volume 1994-1995, page 203.*

[3] *Volume 1999, page 552.*

[4] *Volume 1973-1974, page 379, Volume 1986-1987, page 82 and Volume 1998, page 603.*

[5] *Volume 1992-1993, page 289.*

[6] *Volume 1999, page 552.*

[7] *Volume 2002, page 645.*

[8] *Volume 2000, page 668.*

[9] *Tome VIII, page 9 and Volume 2003, page 123.*

[10] *Tome VIII, page 671 and Volume 1994-1995, page 67.*

[11] *Tome VIII, page 657, Volume 1979-1981, page 365, Volume 1986-1987, page 20, Volume 1994-1995, page 61 and Volume 1996-1997, page 801.*

[12] *Volume 1992-1993, page 223.*

[13] *Volume 1992-1993, page 219 and Volume 2002, page 85.*

[14] *Volume 2002, page 714.*

[15] *Volume 1992-1993, page 223.*

[16] *Volume 1992-1993, page 223.*

[17] *Volume 1992-1993, page 223.*

[18] *Volume 1968-1969, page 462.*

[19] *Volume 2002, page 65.*

[20] *Tome VIII, pages 55 and 57.*

[21] *Volume 2003, page 98.*

[22] *Volume 2003, page 98.*

[23] *Volume 2003, page 98.*

[24] *Volume 2003, page 98.*

[25] *Volume 1992-1993, page 231.*

[26] *Volume 2000, page 670.*

[27] *Volume 2003, page 98.*

[28] *Volume 1992-1993, page 219 and Volume 2002, page 85.*

[29] *Volume 2003, page 98.*

[30] *Volume 2003, page 98.*

[31] *Volume 2003, page 100.*

[32] *Volume 1992-1993, page 219.*

[33] *Volume 1992-1993, page 219.*

[34] *Volume 1992-1993, page 225.*

[35] *Volume 1992-1993, page 224.*

[36] *Volume 2003, page 98.*

[37] *Volume 2002, page 687.*

[38] *Tome VIII, page 62.*
[39] *Volume 1968-1969, page 462 and Volume 1992-1993, page 234.*
[40] *P.89/2003.*
[41] *Volume 2002, pages 65 and 66.*
[42] *P.89/2003.*
[43] *P.89/2003.*
[44] *Volume 2003, page 98.*
[45] *P.89/2003.*
[46] *Volume 2002, page 85.*
[47] *Volume 1992-1993, page 219.*
[48] *Volume 2002, page 714.*
[49] *Volume 2002, page 714.*
[50] *Volume 2003, page 13.*
[51] *Volume 2003, page 98.*
[52] *P.89/2003.*
[53] *P.89/2003.*
[54] *Volume 2003, page 100.*
[55] *P.89/2003.*
[56] *P.89/2003.*