M O N T S E R R A T

NO. 7 OF 2009

ELECTRONIC TRANSACTIONS ACT 2009

ARRANGEMENT OF SECTIONS

PART 5

ELECTRONIC SIGNATURES

PART 6

INFORMATION SECURITY SERVICE PROVIDERS

PART 7

INTERMEDIARIES AND E-COMMERCE SERVICE PROVIDERS

PART 8

DATA PROTECTION

PART 9

MISCELLANEOUS

I ASSENT

Sarita Francis
Governor (Ag.)

DATE: 16.12.2009

M O N T S E R R A T

NO. 7 OF 2009

AN ACT TO ESTABLISH THE LEGAL PRINCIPLES APPLICABLE TO THE CONDUCT OF ELECTRONIC COMMERCE AND THE PROCESSING, VERIFICATION AND ATTRIBUTION OF ELECTRONIC RECORDS; TO PROVIDE FOR THE APPROVAL, REGISTRATION AND LIABILITIES OF SERVICE PROVIDERS; TO ESTABLISH A SYSTEM FOR THE REGULATION OF PROCESSORS OF PERSONAL DATA; AND FOR INCIDENTAL AND CONNECTED PURPOSES.

BE IT ENACTED by the Queen's Most Excellent Majesty, by and with the advice and consent of the Legislative Council of Montserrat and by the Authority of the same as follows:—

PART 1

PRELIMINARY

Short title

1. This Act may be cited as the Electronic Transactions Act 2009.

Interpretation

2. In this Act—

"addressee", in relation to an electronic record, means a person who is intended by the originator to receive the electronic record, but does not include a person acting as an intermediary with respect to that electronic record;

"certificate" means an electronic record which purports to identify a person or entity who, at the time of creation of that record controls a particular signature device;

"data controller" means a person who, either alone or jointly or in common with other persons, determines the purposes for which and the manner in which any personal data is, or is to be, stored, altered, transmitted, distributed, or otherwise processed;

"data processor" means a person who processes personal data on behalf of a data controller;

"deliver" includes give, serve and file;

"e-commerce service provider" means a person who uses electronic means in providing real or personal property, services or information;

"electronic" means (relating to technology) having electrical, magnetic, optical, electromagnetic, or similar capabilities, whether digital, analogue or otherwise;

"electronic agent" means a program, or other electronic or automated means, configured and enabled by a person, that is used to initiate or respond to an electronic record or event in whole or in part, without review by an individual;

"electronic commerce" means the type of business engaged in by e-commerce service providers;

"electronic record" means a record processed and maintained by electronic means;

"electronic signature" means an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record;

"information" includes electronic records, data, text, images, sounds, codes, computer programs, software and databases;

"information processing system" means an electronic system for generating, sending, receiving, storing or otherwise processing information;

"information security service" and **"information security procedure"** includes a service or procedure which is provided to an originator, intermediary or recipient of an electronic record, and which is designed to—

(a) secure that that record can be accessed, or can be put into an intelligible form, only by certain persons; or

(b) secure that—

(i) the authenticity;

(ii) the time of processing; or

(iii) the integrity,

of such a record is capable of being ascertained;

"intermediary", with respect to an electronic record, means a person who sends, receives, stores, processes or provides other services with respect to that electronic record for another person;

"Minister" means the Minister responsible for commerce;

"originator", in relation to an electronic record, means a person who—

(a) sends an electronic record;

(b) instructs another to send an electronic record on his behalf; or

(c) has an electronic record sent by his electronic agent, but does not include—

(i) a person who sends an electronic record on the instructions of another; or

(ii) a person acting as an intermediary with respect to that electronic record;

"personal data" means data which relate to a person who can be identified—

(a) from those data; or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about that person and any indication of the intentions of the data controller or any other person in respect of that person;

"prescribed" means prescribed in Regulations made by the Governor in Council;

"process", in relation to an electronic record, means the creation, generation, sending, transmitting, receiving, storing, communicating, modifying or displaying of the record;

"record" means information that is inscribed, stored or otherwise maintained on a tangible medium or that is stored in an electronic or any other medium and is accessible in a perceivable form;

"signature device" means unique data or a uniquely configured physical device, which is used by the signatory for the purposes of creating an electronic signature;

"transaction" means a transaction whether or not for consideration and whether or not of a commercial nature.

PART 2

LEGAL REQUIREMENTS RESPECTING ELECTRONIC RECORDS

Legal recognition of electronic record

3. Information shall not be denied legal effect or validity solely on the ground that it is—

(a) in the form of an electronic record; or

(b) referred to but not contained in an electronic record that purports to give rise to such legal effect.

Writing

4. (1) Where a document, record or information is required or permitted by any statutory provision or rule of law or by contract or deed to be in writing, or is

described as being written, that requirement, permission or description may be met by information in the form of an electronic record.

(2) Subsection (1) shall apply if the requirement for the document, record or information to be in writing is in the form of an obligation or if the statutory provision or rule of law or contract or deed provides consequences if it is not in writing.

Delivery

5. (1) Where a document, record or information is required or permitted by any statutory provision or rule of law or by contract or deed to be delivered or sent to a person, that requirement or permission may be met by delivery of it in the form of an electronic record if—

(a) the format of the electronic record and the means of delivery is acceptable to the parties; and

(b) where the originator of the electronic record states that the receipt of the electronic record is to be acknowledged, the addressee has knowingly acknowledged the receipt.

(2) Subsection (1) applies whether or not the requirement for delivery or sending is in the form of an obligation or whether or not the statutory provision, rule of law, contract or deed provides consequences for the document, record or information not being delivered or sent.

Original form

6. (1) *(a)* Where a statutory provision, rule of law, contract or deed requires conclusive evidence of the original form of a document, record or information to be presented or retained, that requirement shall be met by the presentation or retention of an electronic record if the document, record or information is accurately represented therein;

(b) Paragraph (a) shall apply if the requirement for the presentation or retention of evidence of the original form of document, record or information is in the form of an obligation or if the statutory provision, rule of law, contract or deed provides consequences if conclusive evidence of the original form of document, record or information is not provided.

(2) *(a)* Where a statutory provision, rule of law, contract or deed requires a document, record or information to be presented or retained in its original form and such document, record or information was first generated in its final form as an electronic record, that requirement shall be met by the presentation or retention of an electronic record if the document, record or information is accurately represented therein;

(b) Paragraph (a) shall apply if the requirement to present or retain the document, record or information in its original form is in the form of an obligation or if the statutory provision, rule of law, contract or deed provides consequences if the original form of the document, record or information is not presented or retained.

(3) For the purposes of subsections (1) and (2) the document, record or information is accurately represented where it has remained complete and unaltered from the time it was first generated in its final form, whether as an electronic record or on any other medium, apart from the application of an information security procedure, or apart from—

(a) the addition of an endorsement; or

(b) an immaterial change;

which arises in the normal course of communication, translation, conversion, storage or display.

Retention of records

7. (1) Where documents, records or information are required by any statutory provision or rule of law or by contract or by deed to be retained, that requirement is met by retaining them in the form of electronic records if—

(a) the information contained in the electronic record is accessible and capable of retention for subsequent reference;

(b) the electronic record is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the document, record or information when it was generated, sent or received;

(c) any information that enables the identification of the origin and destination of an electronic record and the date and time when it was sent and received is retained; and

(d) appropriate steps are taken to ensure the security of such electronic records in compliance with guidelines which may be prescribed.

(2) An obligation to retain documents, records or information, in accordance with subsection (1), does not extend to information the sole purpose of which is to enable the message to be sent or received.

(3) A person may satisfy the requirement referred to in subsection (1) by using the services of another person, if the conditions set out in subsection (1)(a), (b), (c) and (d) are met.

Records available for inspection

8. Where documents, records or information are required by any statutory provision or rule of law or by contract or by deed to be made available for inspection, that requirement shall be met by making such documents, records or information available for inspection in perceivable form as an electronic record.

Admissibility of electronic records

9. In proceedings in a court, tribunal or arbitration, whether of a legal, judicial, quasi-judicial or administrative nature, the admissibility of an electronic record or an electronic signature in evidence shall not be denied solely on the grounds that it is an electronic record or an electronic signature.

Other requirements

10. (1) A requirement in a law for multiple copies of a document to be submitted to a single addressee at the same time is satisfied by the submission of a single electronic record that is capable of being reproduced by that addressee.

(2) An expression in a law, whether used as a noun or verb, including the terms "document", "record", "file", "submit", "lodge", "deliver", "issue", "publish", "write in", "print**"** or words or expressions of similar effect, must be interpreted to include or permit such form, format or action in relation to an electronic record unless otherwise provided for in this Act.

(3) Where a seal is required by law to be affixed to a document and such law does not prescribe the method or form by which such document may be sealed by electronic means, that requirement is met if the document indicates that it is required to be under seal and it includes the electronic signature of the person by whom it is required to be sealed.

PART 3

FORMATION AND VALIDITY OF CONTRACTS

Formation and validity of contracts

11. (1) Unless otherwise agreed by the parties, in the context of the formation of a contract—

(a) an offer;

(b) the acceptance of an offer; and

(c) the method of payment of any consideration payable;

may be expressed by an electronic record.

(2) As between the originator and the addressee of an electronic record, a declaration of intention or other statement shall not be denied legal effect or validity solely on the ground that it is in the form of an electronic record.

PART 4

COMMUNICATION OF ELECTRONIC RECORDS

Attribution of electronic records

12. (1) An electronic record is an originator if it was sent by the originator himself.

(2) As between the originator and the addressee, an electronic record shall be attributable to the originator if it was sent—

(a) by a person who had been authorised by the originator to send the electronic record on his behalf; or

(b) by the originator's electronic agent.

(3) As between the originator and the addressee, an addressee shall be entitled to attribute an electronic record to the originator, and to act on that assumption, if—

(a) in order to ascertain whether the electronic record was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

(b) the electronic record as received by the addressee resulted from the actions of a person whose relationship with the originator, or with any agent of the originator, enabled that person to gain access to a method used by the originator to identify electronic records as his own.

(4) Subsection (3) shall not apply—

(a) as of the time when the addressee has received notice from the originator that the electronic record is not that of the originator and had reasonable time to act accordingly; or

(b) in a case to which subsection (3)(b) applies, at any time when the addressee knew or should have known, had he exercised reasonable care or used any agreed procedure, that the electronic record was not that of the originator.

(5) The addressee shall be entitled to regard each electronic record received as a separate electronic record and to act on that assumption, except to the extent that it duplicates another electronic record and the addressee knew or should have known, had he exercised reasonable care or used any agreed procedure, that the electronic record was a duplicate.

Effect of change or error

13. When a change or error occurs in the transmission of an electronic record—

(a) if the originator and the addressee have agreed to use an information security procedure in respect of the electronic record and one of them has conformed to the procedure, but the other has not, and the nonconforming person would have detected the change or error had he also conformed, the conforming person may avoid the effect of the changed or erroneous electronic record;

(b) an individual who is either the originator or the addressee of an electronic record may avoid the effect of the electronic record if the error was made by the individual in dealing with the electronic agent of another person if the electronic agent did not provide an opportunity for the prevention or correction of the error and, at the time the individual learns of the error, the individual—

(i) promptly notifies the other person of the error and that he did not intend to be bound by the electronic record received by the other person;

(ii) takes reasonable steps, including steps that conform to the other person's reasonable instructions, to return to the other person or, if instructed by the other person, to destroy the consideration received, if any, as a result of the erroneous electronic record; and

(iii) has not used or received any benefit or value from the consideration, if any, received from the other person; and

(c) if neither paragraph (a) nor paragraph (b) applies, the change or error shall have the effect provided by any other law and any contract between the originator and the addressee.

Acknowledgement of receipt of electronic records

14. (1) Subsections (2), (3) and (4) shall apply where, on or before sending an electronic record, or by means of that electronic record, the originator has requested or agreed with the addressee that receipt of the electronic record be acknowledged by the addressee.

(2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by—

(a) a communication by the addressee to the originator, automated or otherwise; or

(b) conduct of the addressee;

that is reasonably sufficient to indicate to the originator that the electronic record has been received.

(3) Where the originator has stated that an electronic record is conditional on receipt by him of an acknowledgement, the electronic record shall be presumed not to have been sent until an acknowledgment has been received by him.

(4) Where the originator has not stated that the electronic record is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator—

(a) may give notice to the addressee—

(i) stating that no acknowledgement has been received and that the electronic record is to be treated as though it had never been sent; or

(ii) specifying a reasonable time by which the acknowledgement must be received; and

(b) if the acknowledgement is not received within the time specified in paragraph (a), may, upon notice to the addressee—

(i) treat the electronic record as though it had never been sent; and

(ii) exercise any other rights the originator may have.

(5) Where the originator receives the addressee's acknowledgement of receipt it may be presumed that the related electronic record has been received by the addressee but that presumption shall not imply that the electronic record received corresponds to the electronic record as sent.

(6) Where the addressee's received acknowledgment states that the related electronic record met technical requirements that the originator and the addressee have agreed should be met, it shall be presumed that the requirements have been met.

(7) Except in so far as it relates to the sending or receipt of an electronic record, this section shall not affect the legal or equitable consequences that may flow either from that electronic record or from the acknowledgement of its receipt.

Time and place of sending and receipt of electronic records

15. (1) An electronic record which is transmitted by electronic means is sent at the time it enters an information processing system outside the control of the originator, his agent, his electronic agent or his agent's electronic agent.

(2) An electronic record which is transmitted by electronic means is received—

(a) in the case where the addressee has designated an information processing system for the purpose of receiving an electronic record—

(i) at the time when the electronic record enters the designated information processing system; or

(ii) if the electronic record is sent to an information processing system of the addressee that is not the designated information processing system, at the time when the electronic record is retrieved by the addressee; or

(b) in the case where the addressee has not designated an information processing system, at the time when the electronic record enters an information processing system of the addressee or is otherwise retrieved by the addressee.

(3) Subsection (2) shall apply notwithstanding that the place where the information processing system is located may be different from the place where the electronic record is deemed to be received under subsection (4).

(4) Subject to subsection (6), an electronic record shall be deemed to have been sent at the place where the originator or his agent has his place of business, and shall be deemed to have been received at the place where the addressee or his agent has his place of business.

(5) For the purposes of subsection (4), if the originator or the addressee has more than one place of business, his place of business is—

(a) that place of business which has the closest relationship to the transaction to which the electronic record relates; or

(b) where there is no transaction to which the electronic record relates—

(i) if he is a body corporate or a registered partnership, his registered office, or

(ii) in any other case, his principal place of business.

(6) Where the originator or the addressee of an electronic record does not have a place of business, or the electronic record does not relate to the originator's business, the electronic record shall be deemed to have been sent or received—

(a) if it is a company, whether established in Montserrat or in any other jurisdiction, at its registered office; or

(b) in any other case, at the place where he ordinarily resides.

PART 5

ELECTRONIC SIGNATURES

Equal treatment of signatures

16. Except as provided in section 17, the provisions of this law shall not be applied so as to exclude, restrict, or deprive of legal effect, any method of creating an electronic signature which—

(a) satisfies the requirements of section 17(1); or

(b) otherwise meets the requirements of an applicable statutory provision, rule of law, contract or deed.

Compliance with a requirement for a signature

17. (1) Where the signature of a person is required by a statutory provision, rule of law, contract or deed, that requirement shall be met in relation to an electronic record if an electronic signature is used that is as reliable as was appropriate for the purpose for which the electronic record was generated or communicated, in all the circumstances, including any relevant agreements.

(2) Subsection (1) applies whether the requirement for a signature is in the form of an obligation or the statutory provision, rule of law, contract or deed provides consequences for the absence of a signature.

(3) An electronic signature shall be reliable for the purpose of satisfying the requirement referred to in paragraph (1) if—

(a) the means of creating the electronic signature is, within the context in which it is used, linked to the signatory and to no other person;

(b) the means of creating the electronic signature was, at the time of signing, under the control of the signatory and of no other person;

(c) any alteration to the electronic signature, made after the time of signing, is detectable; and

(d) where a purpose of the requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

(4) Subsection (3) does not limit the ability of any person—

(a) to establish in any other way, for the purpose of satisfying the requirement referred to in sub-section (1), the reliability of an electronic signature; or

(b) to adduce evidence of the non-reliability of an electronic signature.

Determination of standards

18. The Governor in Council may make regulations prescribing methods which satisfy the requirements of section 17.

Conduct of a person relying on an electronic signature

19. A person relying on an electronic signature shall bear the legal consequences of his failure to—

(a) take reasonable steps to verify the reliability of an electronic signature; or

(b) where an electronic signature is supported by a certificate, take reasonable steps to—

(i) verify the validity, suspension or revocation of the certificate, or

(ii) observe any limitation with respect to the certificate.

Recognition of foreign certificates and electronic signatures

20. (1) In determining whether, or the extent to which, a certificate or an electronic signature is legally effective, no regard shall be had to the place where the certificate or the electronic signature was issued, nor to the jurisdiction in which the issuer had its place of business.

(2) If the Minister considers that the practices of a foreign information security service provider provide a level of reliability at least equivalent to that required of information security service providers in order that they may be approved under section 23, he may, by notice published in the *Gazette*, recognise certificates or classes of certificates issued by the foreign provider as legally equivalent to certificates issued by information security service providers approved under section 23.

(3) The Minister may, by notice published in the *Gazette*, recognise electronic signatures complying with the laws of a foreign jurisdiction relating to electronic signatures as legally equivalent to electronic signatures issued by information security service providers approved under section 23 if the laws of the other foreign jurisdiction require a level of reliability at least equivalent to that required for such electronic signatures under this Act.

(4) The Governor in Council may make regulations prescribing the matters to be taken into account by the Minister when deciding whether to exercise his powers under subsections (2) and (3).

(5) Notwithstanding subsections (2) and (3), parties to transactions may specify that a particular information security service provider, class of information security service providers or class of certificates shall be used in connection with messages or electronic signatures submitted to them.

(6) Where, notwithstanding subsections (2) and (3), the parties to a transaction agree to the use of particular types of electronic signatures and certificates, that agreement shall be recognised as sufficient for the purposes of that transaction.

Notarisation and acknowledgment

21. Where information or a signature, document or record is required by a statutory provision or rule of law, or by contract or deed, to be notarised, acknowledged, verified, or made under oath, the requirement shall be satisfied if, in relation to an electronic signature, electronic document or electronic record, the electronic signature of the person authorised to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the electronic signature, electronic document or electronic record.

PART 6

INFORMATION SECURITY SERVICE PROVIDERS

Register of approved providers

22. (1) The Minister may establish and maintain a register of approved information security services, and of providers of such services, which shall contain particulars of every person who, or service which, is for the time being approved under any arrangements in force under section 23.

(2) The Governor in Council may make regulations prescribing the particulars that are to be included in entries in the register maintained under subsection (1).

(3) The Minister shall—

(a) allow public inspection at all times of an electronic copy of the register; and

(b) publicise any withdrawal or modification of an approval under section 23;

in accordance with arrangements prescribed.

Arrangements for the grant of approvals

23. The Governor in Council may make regulations enabling the Minister to grant approvals, whether subject to conditions or otherwise, on payment of a prescribed fee, to persons who—

(a) are providing information security services in Montserrat or are proposing to do so; and

(b) seek approval in respect of any such services that they are providing, or are proposing to provide, whether in Montserrat or elsewhere.

Restrictions on disclosure of information

24. (1) Subject to subsection (2), information which—

(a) has been obtained under or by virtue of the provisions of this Part; and

(b) relates to the private affairs of any individual or to any particular business;

shall be deemed to be confidential information for the purposes of the Confidential Information Act.

(2) Section 5 of the Confidential Information Act shall not apply to any disclosure of information which is made—

(a) for the purpose of facilitating the carrying out of any functions under this Part, or any prescribed functions, of the Minister;

(b) for the purpose of facilitating the carrying out of prescribed functions of any prescribed person;

(c) in connection with the investigation by the police of a criminal offence or for the purposes of any criminal proceedings; or

(d) for the purposes of any civil proceedings which—

(i) relate to the provision of information security services, and

(ii) are proceedings to which a person approved in accordance with arrangements under section 23 is a party.

(3) If information is disclosed to the public in circumstances in which the disclosure does not contravene the Confidential Information Act, that Act shall not prevent its further disclosure by any person.

Provision of information security services

25. (1) References in this Part, to the provision of an information security service do not include references to the supply of, or of any right to use, computer software or computer hardware unless the supply or the right to use is integral to the provision of information security services which do not consist of such a supply or right to use.

(2) For the purposes of this Part information security services are provided in Montserrat if they are provided from premises in Montserrat and—

(a) they are provided to a person who is in Montserrat when he makes use of the services; or

(b) they are provided to a person who makes use of the services for the purposes of a business carried on in Montserrat or from premises in Montserrat.

Conduct of the information security service provider

26. (1) An information security service provider shall—

(a) act in accordance with the representations it makes with respect to its policies and practices;

(b) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it—

(i) that are relevant to a certificate throughout its life cycle, or

(ii) which are included in a certificate;

(c) provide reasonably accessible means which enable a person who relies on a certificate to ascertain from a certificate—

(i) the identity of the information security service provider,

(ii) that the person who is identified in the certificate had control of the signature device at the time of signing,

(iii) that the signature device was operational on or before the date when the certificate was issued;

(d) provide reasonably accessible means which enable a person who relies on a certificate to ascertain, where relevant, from the certificate or otherwise—

(i) the method used to identify the signature device holder,

(ii) any limitation on the purpose or value for which the signature device or the certificate may be used,

(iii) that the signature device is operational and has not been compromised,

(iv) any limitation on the scope or extent of liability stipulated by the information security service provider,

(v) whether means exist for the signature device holder to give notice that a signature device has been compromised, and

(vi) whether a timely revocation service is offered;

(e) provide a means for a signature device holder to give notice that a signature device has been compromised and ensure the availability of a timely revocation service; and

(f) utilise trustworthy systems, procedures and human resources in performing its services.

(2) An information security service provider who fails to comply with the requirements of subsection (1)—

(a) commits an offence and is liable on conviction to a fine of $10,000 or to imprisonment for a term of 6 months; and

(b) is liable in damages for the loss caused by the failure to a person who reasonably relied on the information security service.

Criteria for determining trustworthiness

27. The Governor in Council may make regulations prescribing the factors to which regard shall be had in determining whether, and the extent to which, systems, procedures and human resources are trustworthy for the purposes of section 26(1)(f).

Contents of a certificate

28. The Governor in Council may make regulations prescribing the matters that shall be specified in a certificate.

Conduct of the signature device holder

29. A signature device holder shall—

(a) exercise reasonable care to avoid unauthorised use of its signature device;

(b) without undue delay, notify any person who may reasonably be expected by the signature device holder to rely on, or to provide services in support of the electronic signature if—

(i) the signature device holder knows that the signature device has been compromised; or

(ii) the circumstances known to the signature device holder give rise to a substantial risk that the signature device may have been compromised; and

(c) where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signature device holder, which are relevant to the certificate throughout its life-cycle, or which are to be included in the certificate.

PART 7

INTERMEDIARIES AND E-COMMERCE SERVICE PROVIDERS

Liability of intermediaries or e-commerce service providers

30. (1) An intermediary or e-commerce service provider may not be subject to any civil or criminal liability in respect of any information contained in an electronic record in respect of which the intermediary provides services, if the intermediary was not the originator of the record and he—

(a) has no actual knowledge that the information gives rise to civil or criminal liability;

(b) is not aware of any facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known, or

(c) follows the procedure set out in section 31 if the intermediary or e-commerce service provider—

(i) acquires knowledge that the information gives rise to criminal liability, or

(ii) becomes aware of facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known.

(2) An intermediary or e-commerce service provider shall not be required to monitor any electronic record processed by means of his system in order to ascertain whether its processing would (apart from this section) constitute or give rise to an offence or give rise to civil liability.

(3) Nothing in this section shall relieve an intermediary or e-commerce service provider from—

(a) any obligation to comply with an order or direction of a court or other competent authority; or

(b) any contractual obligation.

Procedure for dealing with unlawful, defamatory etc. information

31. (1) If an intermediary or e-commerce service provider has actual knowledge that the information in an electronic record gives rise to civil or criminal liability, as soon as practicable the intermediary or e-commerce service provider shall—

(a) remove the information from any information processing system within the intermediary's or e-commerce service provider's control and cease to provide or offer to provide services in respect of that information; and

(b) notify the Minister or appropriate law enforcement authority of the relevant facts and of the identity of the person for whom the intermediary or e-commerce service provider was supplying services in respect of the information, if the identity of that person is known to the intermediary or e-commerce service provider.

(2) If an intermediary or e-commerce service provider is aware of facts or circumstances from which the likelihood of civil or criminal liability in respect of the information in an electronic record ought reasonably to have been known, as soon as practicable the intermediary or e-commerce service provider shall—

(a) follow the relevant procedure set out in a code of conduct approved or standard appointed under section 35 if such code or standard applies to the intermediary e-commerce service provider; or

(b) notify the Minister.

(3) If the Minister is notified in respect of any information under subsection (2), the Minister may direct the intermediary e-commerce service provider to—

(a) remove the electronic record from any information processing system within the control of the intermediary or e-commerce service provider;

(b) cease to provide services to the person to whom the intermediary or e-commerce service provider was supplying services in respect of that electronic record; or

(c) cease to provide services in respect of that electronic record.

(4) An intermediary or e-commerce service provider is not liable, whether in contract, tort, under statute or pursuant to any other right, to any person, including any person on whose behalf the intermediary or e-commerce service provider provides services in respect of information in an electronic record, for any action the intermediary or e-commerce service provider takes in good faith in exercise of the powers conferred by, or as directed by, the Minister under this section.

PART 8

DATA PROTECTION

Data protection

32. (1) The Governor in Council may make regulations prescribing standards for the processing of personal data whether or not the personal data originates inside Montserrat.

(2) Regulations made under subsection (1) may provide for—

(a) the protection of privacy;

(b) the voluntary registration and de-registration to those standards by data controllers and data processors;

(c) the establishment of a register that is available for public inspection showing particulars of data controllers and data processors who have registered or de-registered to those standards and the dates of such registration or de-registration and the countries in respect of which the registration or de-registration applies;

(d) the application of those standards to the countries specified in the regulations;

(e) different standards to be applied in respect of personal data originating from different countries;

(f) such matters as may be necessary or convenient for giving effect to this Part or for its administration.

(3) A data controller or data processor who voluntarily registers to a standard prescribed in regulations made under subsection (1) and who fails to comply with that standard, as it may be amended from time to time, in respect of any personal data originating from a country to which the standard applies that is collected by the data controller during the period of registration, including any time after de-registration is guilty of an offence and is liable on summary conviction to a fine of $10,000, or to imprisonment for 6 months, or to both, and if the offence of which he is convicted is continued after conviction he commits a further offence and is liable to a fine of $5,000 for every day on which the offence is so continued.

Pseudonyms

33. (1) Information security service providers may, at the request of a particular signature device holder, indicate in the relevant certificate a pseudonym instead of the signature device holder's name.

(2) Where a pseudonym is indicated in accordance with subsection (1), the information security service provider shall, where necessary for the investigation by the police of an offence involving the use of electronic signatures, or where otherwise required by law to do so, transfer to a police officer all personal data relating to the signature device holder that is in his possession.

(3) Where personal data is transferred pursuant to subsection (2), the information security service provider shall make a record of the transfer.

(4) The Governor in Council may by regulation prescribe information that is to be provided in addition to the personal data that is to be transferred under subsection (2).

PART 9

MISCELLANEOUS

Consumer Protection

34. (1) A person using electronic communications to sell goods or services to consumers shall provide accurate, clear and accessible information about themselves, sufficient to allow—

(a) the legal name of the person, its principal geographic address, and an electronic means of contact or telephone number;

(b) prompt, easy and effective consumer communication with the seller;

(c) service of legal process.

(2) A person who uses electronic communications to sell goods or services to consumers shall provide accurate and accessible information describing the goods or services offered, sufficient to enable consumers to make an informed

decision about the proposed transaction and to maintain an adequate record of the information.

(3) A person using electronic communications to sell goods or services to consumers shall provide information about the terms, conditions and costs associated with a transaction, and notably—

(a) terms, conditions and methods of payment; and

(b) details of and conditions related to withdrawal, termination, return, exchange, cancellation and refund policy information.

Code of practice

35. (1) The Governor in Council may by regulations establish standards or conduct requirements with which intermediaries or e-commerce service providers carrying on business in or from within Montserrat must comply.

(2) A standard established by regulations made under subsection (1) may relate to one or more of the following matters—

(a) the types of services that are permitted to be provided by intermediaries;

(b) the types of customers to whom services may be provided by intermediaries;

(c) the types of information permitted to be contained in an electronic record for which services are provided by intermediaries;

(d) the contractual application of relevant codes of conduct or standards to customers of intermediaries and e-commerce service providers;

(e) the information to be disclosed by intermediaries and e-commerce service providers including the name, address, e-mail address and contact and registration details;

(f) the actions to be taken in the event of customers of intermediaries or e-commerce service providers sending bulk, unsolicited electronic records;

(g) the practical application of the relevant laws of Montserrat to intermediaries and e-commerce service providers;

(h) procedures for dealing with complaints;

(i) procedures for dispute resolution, including dispute resolution by electronic means;

(j) such other matters as the Governor in Council may require.

(3) Regulations made under subsection (1) shall provide—

(a) that an intermediary or e-commerce service provider who fails to comply with a standard prescribed in the regulations shall in the first instance be given a written warning by the Minister;

(b) that the Minister may direct that person to cease or correct his practices; and

(c) that if that person fails to do so within such period as may be stated in the direction, he commits an offence and shall be liable to such penalties as may be prescribed.

(4) If the Minister is satisfied that a person, body or organisation represents intermediaries or e-commerce service providers carrying on business in Montserrat, the Minister may, by notice given to the person, body or organisation, request that person, body or organisation to—

(a) develop standards or conduct requirements that apply to intermediaries or e-commerce service providers and that deal with one or more specified matters relating to the provision of services by those intermediaries or e-commerce service providers; and

(b) provide details relating to those standards or conduct requirements to the Minister within such time as may be specified in the request.

(5) If the Minister is satisfied with the standards and conduct requirements provided under subsection (4), he shall approve such standards and conduct requirements by notice published in the *Gazette* and thereupon such standards and conduct requirements shall apply to such intermediaries or e-commerce service providers as may be specified in the notice.

(6) If the Minister has approved any standard or conduct requirement that applies to intermediaries or e-commerce service providers, and

(a) he receives notice from a person, body or organisation representing intermediaries or e-commerce service providers or proposals to amend the standard or conduct requirement; or

(b) he no longer considers that the standard or conduct requirement is appropriate,

he may by notice published in the Gazette, revoke or amend any existing standard or conduct requirement.

(7) References in this section to intermediaries and e-commerce service providers include references to a particular class of intermediaries or to a particular class of e-commerce service providers.

Appointment of e-Business Advisory Board

36. (1) The Governor in Council shall appoint a Board, to be known as the e Business Advisory Board—

(2) The Board shall advise the Minister—

(a) on the discharge of the Minister's functions under this Act;

(b) on any matter connected with the functions referred to in paragraph *(a)*;

(c) on any matter connected with the administration of this Act; and

(d) on any matter referred to it by the Minister that is connected or relates to the matters dealt with by this Act.

(3) The members of the Board shall hold office at the pleasure of the Governor in Council and notwithstanding any other enactment may provide their advice on a voluntary basis.

(4) The Board shall consist of not less than seven, or more than ten persons appearing to the Governor in Council to be knowledgeable and experienced about electronic business, the Internet, E-Commerce, technology law or electronic transactions.

(5) The Board shall, at their first meeting, and at the first meeting in every calendar year thereafter, appoint one of their members to be the Chairman of the Board until the date of the first meeting of the Board in the following calendar year.

(6) The Board shall determine its own procedure.

Offences by bodies corporate

37. (1) Where an offence under this Act, which has been committed by a body corporate, is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, any director, manager, secretary or other similar officer of the body corporate, or any person who was purporting to act in any such capacity, he, as well as the body corporate, shall be guilty of that offence and be liable to be proceeded against and punished accordingly.

(2) Where the affairs of a body corporate are managed by its members, subsection (1) shall apply in relation to the acts and defaults of a member in connection with his functions of management as if he were a director of the body corporate.

Regulations

38. (1) Without derogating from the powers to make regulations conferred elsewhere in this Act, the Governor in Council may make regulations—

(a) prescribing matters required or permitted by this Act to be prescribed;

(b) authorising or facilitating—

(i) the investigation of, or

(ii) the bringing of,

criminal proceedings in respect of the processing of electronic records that may be, or is, an offence under this or any other Act;

(c) prescribing the remuneration (if any) to be paid to members of the e-Business Advisory Board;

(d) for carrying the purpose and provisions of this Act into effect.

(2) Regulations made under this Act may provide that the contravention of any provision constitutes an offence and may prescribe penalties for any such offence not exceeding the maximum fine and term of imprisonment prescribed in this Act for any offence under this Act.

Prohibition on key escrow requirements

39. (1) Nothing in this Act shall confer a power on the Governor in Council, or a Minister or public officer—

(a) by conditions of an approval under Part 6; or

(b) by any regulations under this Act;

to impose a requirement on any person to deposit a key for electronic records with another person.

(2) In this section **"key"**, in relation to electronic records, means any code, password, algorithm or other data, the use of which (with or without other keys)—

(a) allows access to the electronic record; or

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

and references in this section to depositing a key for electronic records with a person include references to doing anything that has the effect of making the key available to that person.

Exclusions

40. (1) This Act shall not apply to any rule of law requiring writing or signatures for the creation, execution, variation or revocation of a will or other testamentary instrument.

(2) The Governor in Council may provide by regulations subject to affirmative resolution that this Act, or such of its provisions as may be specified in the regulations, shall not apply to any class of transactions, persons, matters or things.

Variation by agreement

41. The provisions of Part 2, so far as they relate to a contract or deed, and Parts 3, 4 and 5 (except sections 18 and 20(2) to (6)) may be varied or excluded by agreement.

Crown to be bound

42. (1) This Act binds the Crown.

(2) Notwithstanding subsection (1), nothing in this Act obliges any Government Department to generate, send, receive, store or otherwise process any record by electronic means, but either the Minister may, by notice published in the Gazette, indicate that a Government Department will receive and process electronic records relating to such matters as may be specified in the notice.

(3) Until a notice under subsection (2) shall have been published, no person dealing with such Government Department shall be entitled, by means of an electronic record, to satisfy a requirement to process a record.

SPEAKER

Passed the Legislative Council this 24th day of November, 2009.

CLERK OF COUNCILS

THE ELECTRONIC TRANSACTIONS BILL, 2009

EXPLANATORY MEMORANDUM

The objects of this Bill are -

(a) to facilitate modern business and commerce in Montserrat;
(b) to facilitate electronic transactions on a technology neutral basis by means of reliable electronic records;
(c) to remove uncertainties in relation to conducting transactions electronically with respect to the requirements for documents and for signatures to be in writing;
(d) to promote public confidence in the validity, integrity and reliability of conducting transactions electronically; and
(e) to promote the development of the legal and business infrastructure necessary to implement electronic transactions securely.

The Bill will provide that transactions carried out by electronic means are regulated in a manner that –

(a) permits and encourages the growth of business by electronic means through the operation of free market forces;
(b) promotes the greatest possible use of industry self-regulation;
(c) is flexible; and
(d) is technologically neutral.

Clause 3 provides that the use of electronic communication shall not, by itself, invalidate a communication or its contents. This clarifies the legal recognition of electronic communication.

Clause 4 provides that any document, apart from those excepted in clause 1, which can be in writing, will be just as valid if it is in electronic form.

Clause 5 provides that a document that is required to be delivered to a person will be validly delivered if it is sent electronically. The format of the electronic record and the manner of delivery must be acceptable to both parties.

Clause 6 sets out the circumstances where a document that is required to be presented or retained in its original form, or where evidence of the original form of a document is required, those requirements can be satisfied by an electronic version of the document.

Clause 7 sets out the conditions to be complied with if a requirement to retain a document is to be satisfied by the retention of an electronic version.

Clause 8 provides that a requirement to make documents available for inspection shall be satisfied if a perceivable electronic version is produced.

Clause 9 ensures that courts, tribunals, etc. shall not be able to deny admissibility of documents solely on the grounds that they are presented in evidence in electronic form.

Clause 10 makes provision for where multiples copies are required by law, and allows for the use of electronic seals.

Clause 11 enables contracts to be concluded in electronic form.

Clause 12 deals with the attribution of electronic messages.

Clause 13 deals with the situation where there is a change or error in the transmission of an electronic record.

Clause 14 makes provision to govern the validity of acknowledgements of electronic messages and the circumstances where an electronic message may be presumed to have been received.

Clause 15 sets out the presumptions to be made about the time and place of sending and receipt of electronic messages.

Clause 16 ensures that preference is not given to any particular method of digitally signing an electronic message.

Clause 17 provides that where a document has to be signed, if the document is in electronic form it may be digitally signed. It then provides a number of conditions that have to be complied with if the electronic signature is to be reliable for the purposes of the Act.

Clause 18 enables regulations to be made prescribing methods which satisfy the requirements of clause 17.

Clause 19 prescribes the legal consequences of a person who fails to verify, in accordance with the procedures set out, an electronic signature.

Clause 20 makes provision for the conditions that have to be complied with before a foreign electronic signature, or the certificate attached thereto, shall be recognised.

Clause 21 provides that where information or a signature, document or record is required by a statutory provision or rule of law, the electronic signature of the person authorised to perform those acts, together with all other information

required to be included by other applicable law, is attached to or logically associated with the electronic signature, electronic document or electronic record.

Clause 22 creates an obligation for the keeping of a register of approved providers.

Clause 23 provides that the Governor in Council may by regulations grant approvals to persons who are providing information security services in Montserrat.

Clause 24 Provides that section 5 of the Confidential Information Act shall not apply to any disclosure of information which is made in connection with the investigation of a criminal offence and for the purposes of any civil proceedings which relate to the provision of information security services,

Clause 25 defines the provision of information security services.

Clause 26 sets out several provisions relating to the conduct of the information security service provider. An information security service provider must act in accordance with the representations it makes with respect to its policies and practices; exercise reasonable care to ensure the accuracy and completeness of all material representations made by it , provide reasonably accessible means which enable a person who relies on the certificate to ascertain, where relevant, from the certificate or otherwise, provide a means for a signature device holder to give notice that a signature device has been compromised and ensure the availability of a timely revocation service; and utilise trustworthy systems, procedures and human resources in performing its services. An information security service provider shall be liable for its failure to satisfy these requirements.

Clause 27 provides that the Governor in Council may make regulations regarding the criteria for determining trustworthiness, of the procedures and human resources of information security service provider in performing their services

Clause 28 specifies that the Governor in Council may make regulations prescribing the matters that shall be specified in a certificate.

Clause 29 sets out the duties ad responsibilities of a signature device holder in terms of conduct.

Clauses 30 and 31 set out matters that limit the liability of intermediaries and service providers as defined in the Bill.

Clause 32 gives the Governor in Council the power to make regulations prescribing standards for the processing of personal data whether or not the personal data originates inside Montserrat.

Clause 33 provides that information security service providers may, at the request of a particular signature device holder, indicate in the relevant certificate a pseudonym instead of the signature device holder's name.

Clause 34 makes basic provisions for consumer protection for online transactions. The provisions are adapted from the OECD Guidelines for Consumer Protection in the context of Electronic Commerce.

Clause 35 enables the prescription of a Code of Practice to provide standards and other requirements that have to be complied by intermediaries and service providers.

Clause 36 requires the appointment of an e-Business Advisory Board.

Clause 37 defines the situation, which arises when an offence is committed by a body corporate.

Clause 38 is a general power to make regulations.

Clause 39 Prohibits the Governor in Council, or a Minister or official member from imposing a requirement on any person to deposit a key for electronic records with another person.

Clause 40 provides that the bill when passed shall not apply to any rule of law requiring writing or signatures for the creation, execution, variation or revocation of a will or other testamentary instrument.. This clause also allows the Governor in Council to provide by regulations that the Act shall not apply to any class of transactions, persons, matters or things.

Clause 41 enables parties to transactions to agree that certain sections shall not apply or shall apply with amendments.

Clause 42 provides that the law shall apply to the Crown. It also provides that, in respect of government business, electronic communications may only be validly used by the public after notice to that effect has been published.

Attorney General