

DRAFT MODEL LAW ON ELECTRONIC EVIDENCE

1. Law Ministers and Attorney-Generals of Small Commonwealth Jurisdictions, at their 2000 meeting, recognized that common law rules of evidence were not adequate to deal with technological advances and needed to be modernised. They welcomed the convening of an Expert Group to develop model legislation on electronic evidence to address the needs of small Commonwealth jurisdictions.

2. The Expert Group examined the admissibility of electronic evidence and the question whether the rules that apply to other forms of documentary evidence can be applied in a like manner to electronic documents. Computer records are sophisticated systems that may be more prone or vulnerable to alteration and degradation than are records on paper. Therefore it was thought that the admissibility rule should take account of this risk. The Group noted that most jurisdictions seeking to impose a minimum level of reliability for admissibility of documents do so by focusing not on the document itself but rather on the method (system) by which the document was produced. This is because it is very difficult to show anything about the electronic document per se. By showing the reliability of the system one can lay the basis for admissibility of the document which is the product of that system. The Group agreed that system reliability is the most sensible measurement.

3. The model law contains provisions on general admissibility, the scope of the model law, authentication, application of best evidence rule, presumption of integrity, standards, proof by affidavit, cross examination, agreement on admissibility of electronic records, and admissibility of electronic signature.

4. On the basis of these deliberations, the Commonwealth Secretariat decided that because of the complexity of the issues, a separate model law on electronic evidence should be drawn up in order to ensure admissibility of such evidence. The model law draws on the Singapore Evidence Act Section 35 (1), the Canada Uniform Electronic Evidence Act and UNCITRAL Model Law on E-Commerce. Member countries wishing to make use of the model E-Evidence Law may choose to do so as –

- a separate piece of legislation; or
- part of a law on electronic transactions; or
- as amendments to existing laws on evidence; or
- as an addition to the proposals contained in paper **LMM(02)4** which deals with modernisation of evidence laws but concentrates primarily on criminal law matters and business records in their more traditional sense.

5. The model provisions on electronic evidence are annexed to this paper.

ACTION BY LAW MINISTERS

6. Law Ministers may wish to endorse the annexed Electronic Evidence Model Law and commend it to member countries for adoption (or adaptation to national circumstances) as a Commonwealth model of good practice.

Commonwealth Secretariat
Marlborough House
London SW1Y 5HX

September 2002

ELECTRONIC EVIDENCE MODEL LAW

AN ACT to make provision for the legal recognition of electronic records and to facilitate the admission of such records into evidence in legal proceedings.

BE IT ENACTED by the Parliament [*name of legislature*] of [*name of country*] as follows:

- Short Title 1. This Act may be cited as the Electronic Evidence Act, 2002
- Interpretation 2. In this Act,

 “data” means representations, in any form, of information or concepts;

 “electronic record” means data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, print out or other output of that data.

 “electronic records system” includes the computer system or other similar device by or in which data is recorded or stored, and any procedures related to the recording and preservation of electronic records.

 “legal proceeding” means a civil, criminal or administrative proceeding in a court or before a tribunal, board or commission.
- General 3. Nothing in the rules of evidence shall apply to deny the admissibility of
Admissibility an electronic record in evidence on the sole ground that it is an electronic record.

 4. (1) This Act does not modify any common law or statutory rule relating to the admissibility or records, except the rules relating to authentication and best evidence.
- Scope of Act (2) A court may have regard to evidence adduced under this Act in applying any common law or statutory rule relating to the admissibility of records.
- Authentication 5. The person seeking to introduce an electronic record in any legal proceeding has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.

Application
of Best
Evidence
Rule

6. (1) In any legal proceeding, subject to subsection (b), where the best evidence rule is applicable in respect of electronic record, the rule is satisfied on proof of the integrity of the electronic records system in or by which the data was recorded or stored.

(2) In any legal proceeding, where an electronic record in the form of printout has been manifestly or consistently acted on, relied upon, or used as the record of the information recorded or stored on the printout, the printout is the record for the purposes of the best evidence rule.

Presumption
of Integrity

7. In the absence of evidence to the contrary, the integrity of the electronic records system in which an electronic record is recorded or stored is presumed in any legal proceeding:

- (a) where evidence is adduced that supports a finding that at all material times the computer system or other similar device was operating properly, or if not, that in any respect in which it was not operating properly or out of operation, the integrity of the record was not affected by such circumstances, and there are no other reasonable grounds to doubt the integrity of the record.
- (b) where it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or
- (c) where it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

Standards

8. For the purpose of determining under any rule of law whether an electronic record is admissible, evidence may be presented in respect of any standard, procedure, usage or practice on how electronic records are to be recorded or preserved, having regard to the type of business or endeavour that used, recorded or preserved the electronic record and the nature and purpose of the electronic record.

Proof by
Affidavit

9. The matters referred to in sections 6, 7, and 8 may be established by an affidavit given to the best of the deponent's knowledge or belief.

Cross
Examination

10. (1) A deponent of an affidavit referred to in section 9 that has been introduced in evidence may be cross-examined as of right by a party to the proceedings who is adverse in interest to the party who has introduced the affidavit or has caused the affidavit to be introduced.

(2) Any party to the proceedings may, with leave of the court, cross-examine a person referred to in subsection 7(c).

Agreement on
Admissibility
of Electronic
Records

11. (1) Unless otherwise provided in any other statute, an electronic record is admissible, subject to the discretion of the court, if the parties to the proceedings have expressly agreed at any time that its admissibility may not be disputed.

(2) Notwithstanding subsection (1), an agreement between the parties on admissibility of an electronic record does not render the record admissible in a criminal proceeding on behalf of the prosecution if at the time the agreement was made, the accused person or any of the persons accused in the proceeding was not represented by a solicitor.

Admissibility
of Electronic
Signature

12. (1) Where a rule of evidence requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law or avoids those consequences.

(2) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a person, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of the person.