Expert group recommends e-commerce legal framework

Mark Sneddon, a member of the Attorney-General's Expert Group on Electronic Commerce, outlines the report's major recommendations

The Federal Attorney-General's Expert Group on Electronic Commerce presented its report, "Electronic Commerce: Building the Legal Framework" on March 31, 1998. The report was released for public comment up until the end of May 1998. Thereafter, the federal government has to make a decision on whether to legislate as recommended in the report.

The Expert Group was appointed in July 1997. It was chaired by an officer of the Attorney-General's Department and comprised experts from industry, business and the legal profession, including this author. The terms of reference required the Group to:

- identify the nature and magnitude of the legal problems that must be addressed to facilitate electronic commerce; and
- determine a preferred option, if any for regulation of electronic transactions taking account of the goals of transaction efficiency, minimising regulatory burdens, resolving legal uncertainties and the desirability of uniform legislation and conformity with existing international standards and uniform rules (in particular the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce).

The Expert Group's report recommends federal legislation to remove existing legal obstacles to electronic transactions and to reduce the legal uncertainty surrounding the use of electronic messages and electronic signatures for transactions. The report recommends that the legislation should be broad in its operation, covering all data messages in trade and commerce and all data messages used in transactions with government (eg. tenders, permit applications, filing, benefits processing), subject to some categories of exceptions being developed (possible examples include wills, negotiable instruments and some consumer transactions).Three broad aims underpin the report:

- Functional Equivalence - as far as possible paper-based commerce and electronic commerce should be treated equally by the law;
- Technology Neutrality - the law should not discriminate between forms of technology
- Facilitate international harmonisation and standards - by broadly following the framework of the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce with some amendments.

Following these aims, the report does not try to pick technological winners or prescribe detailed rules for particular technologies, such as digital signatures relying on asymmetric public key encryption and certification authorities. In other jurisdictions which have legislated to give digital signatures some legal preference over other authentication methods, such as Utah and Malaysia, the legislation has had to be highly prescriptive as to standards in order to responsibly confer preferential legal benefits. The market has so far been reluctant to utilise these prescriptive regimes. On the contrary, certification authority businesses have emerged in jurisdictions without prescriptive and preferential legal rules.

The report follows the framework of the United Nations Commission on International Trade Law Model Law on Electronic Commerce and recommends the adoption of provisions based on the Model Law with some amendments and omissions. The main recommendations of the report are as follows:

- Legal Effect: information, records, signatures, messages and contracts are not to be denied legal effect solely on the ground that they are in electronic form.
- Writing: information in the form of an electronic data message is sufficient to satisfy any legal requirement that information be in writing.
- Signature: where the law requires the signature of a person, that requirement is met in relation to an electronic data message if a method is used to identify that person and to indicate their approval of the contents of the message, and that method is as reliable as was appropriate for the purpose (e.g. a password, PIN or digital signature)
- Originals: legal requirements for information to be presented or retained in its original form are satisfied by an electronic form of that information which can be displayed and which reliably assures the integrity of the information
- Evidence: information in the form of an electronic data message is not to be denied admissibility in evidence on the sole ground that it is a data message
- Record Retention: Legal requirements for retaining records (e.g. under tax or corporations law) can be satisfied by

... continued next page

... continued from previous page

retaining electronic data messages subject to satisfying conditions of reliability and identification of place, time and date of origin and receipt.

• Time and Place of Dispatch and Receipt: rules are proposed to make certain when and where electronic messages are sent and received (e.g. at anISP's server or in an electronic mailbox or when read).

• Forged Signatures and Altered Messages: the common law position applies that a person is bound by a message which is sent by that person or with their authority. Following the principle of functional equivalence with paper-based commerce, no special legislative rules are created to presume the attribution of a message to the apparent sender and the non-alteration in transit of data messages.

• Parties can manage the commercial risks of forged signatures and alteration of messages by using suitably reliable technology and, in the case of parties who regularly exchange messages, by agreeing on risk allocation rules in their trading partner agreements. However, to avoid parties in significantly disadvantaged bargaining positions having unfair attribution and risk allocation rules imposed on them through contract, the report recommends that a party cannot rely on agreed rules of message attribution (including message integrity) unless it is fair and reasonable to do so in all the circumstances (similar to s.68A(3) of the Trade Practices Act). A non-exhaustive list of the factors relevant to fairness and reasonableness should include the reliability and security of the authentication and message integrity procedures used (eg PIN, digital signature or biometrics) and the access device used to operate those procedures (eg chip card and PIN).

The report seeks to facilitate electronic commerce at a fundamental level by removing legal obstacles and reducing uncertainty and legal risk. Other government reports and initiatives with more specific applications complement the Expert Group's work:

1) The National Public Key Infrastructure Working Group operating under the auspices of the National Office on the Information Economy is overdue to report on the structure of a public key authentication framework (PKAF) for digital signatures and certification authorities based on the specific authentication technology of public/private key encryption.

2) Project Gatekeeper, within the federal Office of Government Information Technology, was launched on May 6, 1998. It proposes a whole list of government public key infrastructure for the use of digital signatures for communications with and within the federal government.

3) There is a large amount of work being done on the adaptation or application of existing regulatory regimes to electronic transactions in particular fields such as tax, company law, consumer protection and privacy.

The full report of the Expert Group including an Executive Summary is available at http://law.gov.au/aghome/advisory/eceg/ecegreport.html

Mark Sneddon is Associate Professor of Law at the University of Melbourne, a solicitor, and consultant to Clayton Utz

Principles for Consumer Protection in Electronic Commerce

The National Advisory Council on Consumer Affairs has released a set of 12 principles to help in improving consumer protection in the electronic commerce marketplace.

1. Protection: consumers using electronic commerce are entitled to at least the same levels of protection as provided by the laws that apply to existing forms of commerce.

2. Identification: consumers should be able to establish the identity and location of businesses with whom they deal.

3. Information: consumers should have readily available clear and comprehensive information before and after any purchase of goods and/or services.

4. Clarity: sellers must state contract terms in clear, simple language.

5. Confirmation: sellers should ensure they receive confirmed meaningful consent from consumers for a purchase of goods and/or services.

6. Payment: consumers are entitled to receive clear information about the types of payments which will be accepted by the merchant or the payment provider.

7. Complaints procedure: consumers are entitled to have their complaints and inquiries dealt with fairly and effectively.

8. Dispute Resolution: sellers should provide information to consumers about affordable and effective dispute resolution arrangements, where they are available.

9. Privacy: sellers must respect customer privacy.

10. Code Compliance: industry code administration bodies must closely monitor the application and effectiveness of their codes and be able to correct any deficiencies which are identified.

11. Confidence: each code operating body should strive to maintain and promote consumer confidence in the global marketplace.

12. Regulation: governments should actively develop their consumer protection responsibilities.

The principles were developed with reference to the UN Guidelines for