E 3168

LAW·COMMISSION
TE·AKA·MATUA·O·TE·TURE

Report 68

Electronic Commerce Part Three

Remaining Issues

December 2000
Wellington, New Zealand

The Law Commission is an independent, publicly funded, central advisory body established by statute to undertake the systematic review, reform and development of the law of New Zealand. Its purpose is to help achieve law that is just, principled, and accessible, and that reflects the heritage and aspirations of the peoples of New Zealand.

The office of the Law Commission is at 89 The Terrace, Wellington
Postal address: PO Box 2590, Wellington 6001, New Zealand
Document Exchange Number: SP 23534
Telephone: (04) 473–3453, Facsimile: (04) 471–0959
Email: com@lawcom.govt.nz
Internet: www.lawcom.govt.nz

Report/Law Commission, Wellington, 2000
ISSN 0113–2334 ISBN 1–877187–63–1
This report may be cited as: NZLC R68
Also published as Parliamentary Paper E 3168*

This report is also available on the internet at the Commission's website: http://www.lawcom.govt.nz

---

* Previous Law Commission reports have been published as Parliamentary Papers E 31AA–E 31AZ. In this and future reports, the figures AA–AZ shall be replaced by the report number; in this instance, 68.

Contents

20 December 2000

Dear Minister

I am pleased to submit to you Report 68 of the Law Commission, *Electronic Commerce Part Three: Remaining Issues*.

Yours sincerely

The Hon Justice Baragwanath
President

The Hon Phil Goff
Minister of Justice
Parliament Buildings
Wellington

The Hon Margaret Wilson
Associate Minister of Justice and Attorney-General
Parliament Buildings
Wellington

Preface

THIS IS THE FINAL REPORT to be issued by the Law Commission on the International Trade Project which was started in October 1997.[1] The Commission has, as part of that project, published the following reports and study papers: *Electronic Commerce Part 1: A Guide for the Legal and Business Community*[2] (ECom 1); *Cross-Border Insolvency: Should New Zealand Adopt the UNCITRAL Model Law on Cross-Border Insolvency?*;[3] *Electronic Commerce Part 2: A Basic Legal Framework*[4] (ECom 2), and *International Trade Conventions*.[5] The Commission has also addressed criminal law issues affecting electronic commerce in *Computer Misuse*[6] which was supplemented by chapter 12 of ECom 2.

The Commission wishes to record its thanks to the members of its Electronic Commerce Advisory Committee, all of whom have given generously of their time in assisting the Commission with its work. Members of the Committee are Elizabeth Longworth, Barrister and Solicitor of Longworth Associates, Auckland; David Goddard, Barrister, Wellington; Jim Higgins, Managing Director, The Networking Edge Limited, Wellington and Dr Henry Wolfe of the Information Science Department of the University of Otago. The Commission also records its thanks to David Goddard for his services in representing New Zealand so ably at meetings of the Hague Conference on Private International Law, where conflict of law issues of the type discussed in chapter 3 have been aired internationally.

---

1 See Law Commission *Electronic Commerce Part 1: A Guide for the Legal and Business Community*: *NZLC R50* (Wellington, 1998) ix.

2 Law Commission, above n 1.

3 Law Commission, *NZLC R52* (Wellington, 1999).

4 Law Commission, *NZLC R58* (Wellington, 1999).

5 Law Commission, *NZLC SP5* (Wellington, 2000).

6 Law Commission, *NZLC R54* (Wellington, 1999).

The Commission would also like to thank Reg Hammond and Andrew McCallum of the IT Policy Group within the Ministry of Economic Development for their co-operation and assistance in the Commission's international trade work.

From its inception in October 1997 until May 1999, the Commissioner in charge of the International Trade Project was DF Dugdale. From May 1999 the Commissioner in charge of the project has been Paul Heath QC. The research for this report has been undertaken by Lucy McGrath and Karen Belt, to whom the Commission expresses its appreciation. The Commission also takes this opportunity to acknowledge the assistance of other researchers who contributed to the International Trade Project and who are no longer with the Commission; in particular, Nicholas Russell, Megan Leaf and Jason Clapham.

This report is also available from the Commission's website: www.lawcom.govt.nz

---

Summary of recommendations

- New Zealand should recommend that the Hague Conference on Private International Law consider what principles should be applied when determining the applicable law in cross-border commercial disputes (paragraphs 28–30);
- the Ministry of Justice and the Ministry of Foreign Affairs and Trade should continue to monitor the international initiatives in progress dealing with cross-border computer-related offences (paragraphs 33–39);
- New Zealand should continue to be involved in the work of international forums working toward the harmonisation of privacy and data protection laws (paragraphs 52–59);
- the New Zealand Bankers' Association should take into account the problems identified by the Banking Ombudsman, and Australian developments in risk allocation for unauthorised transactions, when conducting its review of the Code of Banking Practice in 2001 (paragraphs 67–69);
- as previously recommended, the definition of "distributor" in section 2(1) of the Defamation Act 1992 should be amended to include an explicit reference to an Internet Service Provider (ISP)(paragraph 80);
- the Commission recommends that overseas developments in regulating internet content by imposing liability on ISPs be kept under review by the Ministry of Justice (paragraphs 82–95);
- the Ministry of Economic Development should monitor the enactment in other countries of article 12 of the draft United Nations Commission on International Trade Law (UNCITRAL) draft Model Law on Electronic Signatures, to determine whether it may be desirable for New Zealand to enact a cross-border recognition provision at some stage in the future (paragraphs 120–123).

1
Introduction

1 THE PURPOSE OF THIS REPORT is to address the questions posed in ECom 2 and, where appropriate, to refer to developments on other topics since publication of ECom 2. In summary, those questions were:

- In relation to the allocation of liability for unauthorised electronic banking transactions (both credit card and electronic funds transfer (EFT) transactions):
  - should parties be left to contractual devices, notwithstanding disproportionate bargaining powers;
  - if not, how should risk be allocated between the parties; and
  - should rules for allocating risk be included in legislation or, if not, form part of a voluntary industry code?
- In relation to the privacy issues raised by caching:
  - are there any practical problems or issues arising from the application of the existing law;
  - if so, do those problems arise in relation to collecting, holding or giving access to information; and
  - if a law change is warranted, how might that amendment be framed?
- In general, is legislation required to allow the use of transportation documents in an electronic form?
- In relation to civil remedies for the misuse of information:
  - are the existing statutory, common law and equitable actions sufficient to meet the needs of those involved in electronic commerce;
  - if not, should information be redefined as property; or
  - should we codify the law of unjust enrichment; or
  - should a statutory tort be introduced which would give the owner of a computer system a right of action against a person where that person had breached criminal legislation dealing with computer misuse and, as a result, caused loss or obtained benefit; and, if so
  - will the New Zealand insurance market provide adequate and cost-effective cover for electronic commerce risks for businesses operating in electronic commerce?

- What other solutions are being suggested to deal with the issues raised?

2 The Commission has, previously, in ECom 1 and ECom 2, set out the principles which it has applied in its work on electronic commerce.[7] For more detail, readers are referred to those reports. In general terms, it will now be left to Government agencies to deal with outstanding issues.

3 In consequence of the recommendations made by the Commission in ECom 2, an Electronic Transactions Bill was introduced into Parliament on 31 October 2000.[8] Generally, the Electronic Transactions Bill follows the recommendations set out in ECom 2. There are, however, some policy differences which are addressed in chapters 1 and 9 of this report. Policy was developed further after consultation undertaken with interested parties earlier this year by the Ministry of Economic Development.

4 While the Electronic Transactions Bill does not deal with the law of evidence, the Commission has been advised by the Ministry of Justice[9] that the Evidence Code recommended in its report *Evidence: Reform of the Law*[10] will be the subject of a legislative bid in 2001. In our view, the Code will deal adequately with electronic commerce issues. There is likely to be an interval between the time at which the Electronic Transactions Bill and the Evidence Code come into force. In the Commission's view, as long as the interval between enactment of the two statutes is short it can be managed adequately. As it is intended that the Evidence Code will apply to all hearings commenced after the date on which it comes into force, any disputes involving the Electronic Transactions Act (once passed) are unlikely to reach a substantive hearing prior to enactment of the Evidence Code, if that interval is short. Any unforeseen delay in the introduction of the Code could, however, be problematic.[11]

---

7 See ECom 1, paras 28–45 and ECom 2, paras 9–10.

8 The Bill is set out in full in appendix A.

9 Correspondence with Ministry of Justice, 23 October 2000.

10 Law Commission *NZLC R55 – Vol 1* (Wellington, 1999); see also ECom 2, chapter 7.

11 See s 5(3) of the Draft Evidence Code set out in *Evidence: Evidence Code and Commentary: NZLC R55 – Vol 2,* 26.

5 We note that in addition to the civil law issues there are still criminal law issues to be addressed – these are the subject of a Supplementary Order Paper introduced into Parliament on 7 November 2000. Some comments on the criminal law issues are to be found in chapter 4 of this report.

6 Another matter which requires public consultation and debate is the topic of security and encryption.[12] While no public discussion paper has yet been issued, we are told that such a paper will be produced next year. As noted in ECom 2,[13] submissions can be made to the Chairman, National Cryptography Policy Committee, Domestic and External Security Secretariat, Department of Prime Minister and Cabinet, Executive Wing, Parliament Buildings, Wellington.

---

[12] ECom 2, chapter 10.

[13] ECom 2, para 164.

2
The Electronic Transactions Bill

Background

7 THE ELECTRONIC TRANSACTIONS BILL was introduced into Parliament on 31 October 2000. In large measure it seeks to implement the recommendations made by the Commission in ECom 2. This chapter:

- explains the structure of the Electronic Transactions Bill as introduced into Parliament;
- notes which of the recommendations made in ECom 2 are included in the Bill and which are not; and
- identifies policy changes which have occurred since the Commission published its recommendations in ECom 2.

The Electronic Transactions Bill is reproduced in full in appendix A.

8 We note that the topic of electronic signatures has been addressed in the Bill in a more comprehensive way than has been done in other jurisdictions.[14] Greater predictability in the assessment of the reliability of electronic signatures can be expected from the way in which the Bill is framed, as it draws upon the draft UNCITRAL Model Law on Electronic Signatures.[15] While the draft Model Law requires formal approval from the United Nations

[14] A summary of legislation dealing with electronic commerce issues throughout the world and based, by and large, upon the UNCITRAL Model Law on Electronic Commerce, is set out in appendix D.

[15] The draft UNCITRAL Model Law on Electronic Signatures (to which reference was made in ECom 2, chapter 9, under its working title of draft "Uniform Rules") was finalised at the last session of the UNCITRAL Working Group on Electronic Commerce held in Vienna in September 2000. New Zealand was represented at that session by Commissioner Paul Heath QC. The full text of the draft Model Law is set out in full in appendix B.

Commission on International Trade Law in plenary session (expected in June 2001) and adoption by the General Assembly of the United Nations, it is clear that the added predictability arising out of article 6 of the draft Model Law (in substance, to be found in clause 24 of the Bill) will add value to article 7 of the Model Law on Electronic Commerce, on which the laws of many of our trading partners are based.[16] A discussion of the draft Model Law on Electronic Signatures is contained in chapter 9.

9 One important difference between the Electronic Transactions Bill and the recommendations made in ECom 2 should be noted at the outset. In the Executive Summary of ECom 2[17] we said:

> In general terms, enactment of an Electronic Transactions Act will provide a basic legal framework to facilitate trade and to remove barriers to trade being carried on electronically. We have deliberately restricted our recommended legislation to "trade" related transactions for the reasons given at paragraph 34.

At paragraph 34 of ECom 2 we expressed the view that confining the Electronic Transactions Act to electronic transactions conducted "in trade" would avoid the need to list individually many of the legal requirements which should be excluded from the application of the Act, such as wills and affidavits and the delivery of Government services. However, as a result of consultation which has occurred since ECom 2, the Government has decided to apply the Electronic Transactions Act to all types of electronic transactions (including those relating to the delivery of Government services) unless specifically excluded by the Act.

Structure of the Bill

10 The Electronic Transactions Bill is divided into three parts.

- Part 1 of the Bill deals with a number of preliminary matters in clauses 3–7. Of particular importance are clause 3 (the purpose of the Act), clause 5 (definitions) and clause 6 (relating to the use of UNCITRAL documents[18] to interpret the Act). Clause 7 provides that the Act will bind the Crown.

---

16 Generally, see appendix D.

17 ECom 2, para E4.

18 A similar provision can be found in s 3 of the Arbitration Act 1996.

- Part 2 of the Bill is designed to improve certainty in the application of the law to electronically generated information and to electronic communications. The provisions in part 2 relate to the validity of electronically generated information (clause 8) and contain default rules concerning the dispatch and receipt of electronic communications (clauses 9–13).
- Part 3 of the Bill is divided into three subparts and deals with the application of particular legal requirements to electronic transactions.
  - Subpart 1 (clauses 14–17) provides general rules concerning the transactions covered by the Bill (clause 14), the satisfaction of legal requirements and the use of electronic technology (clause 15), the consent to the use of electronic technology (clause 16) and a definition of the circumstances in which the integrity of information is maintained in electronic form for the purposes of part 3 of the Bill (clause 17).
  - Subpart 2 deals with legal requirements for writing (clauses 18–21), signatures (clauses 22–24) and retention of documents (clauses 25–27). Clauses 28–31 deal with legal requirements for the provision, production of and access to certain types of information (in both electronic and non-electronic forms), while clause 32 deals with the legal requirement for an original document.
  - Subpart 3 contains miscellaneous provisions (clauses 33–36) to which reference will be made later.

11 The purpose of the Electronic Transactions Bill is stated in clause 3 as being to facilitate the use of electronic technology by reducing uncertainty regarding the legal effect of information that is in electronic form, or is communicated by electronic means, and regarding the time, place and despatch and receipt of electronic communications, and by providing that certain paper-based legal requirements can be met by using electronic technology that is the functional equivalent of the paper-based requirement. This overall purpose is broadly consistent with the nature of the basic legal framework which this Commission recommended in ECom 2, paragraphs 4–10. The purpose is also consistent with the thrust of the UNCITRAL Model Law on Electronic Commerce.[19]

---

[19] Generally, see the *Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce* (1996), paras 15–18, reproduced in ECom 2, 165–167.

Comparison of Electronic Transactions Bill with recommendations in ECom 2

12 Recommendations for the enactment of an Electronic Transactions Act to remove immediate barriers to electronic commerce were set out in paragraphs 332–337 of ECom 2. It is unnecessary for present purposes to address the additional matters raised in paragraphs 338–341 of ECom 2.

13 With regard to the recommendations made in paragraph 333 of ECom 2, we note:

- Clause 9(a) of the Bill contains a provision akin to article 4 of the Model Law, which preserves party autonomy in electronic communications. Clauses 8(a) and (b) respectively enact articles 5 (regarding non-discrimination) and 5 bis (regarding incorporation by reference) of the Model Law.
- The Electronic Transactions Bill contains an equivalent to article 7 of the Model Law on Electronic Commerce which deals with electronic signatures. Under clause 24 of the Bill, greater predictability in relation to the reliability of electronic signatures is brought about through the use of a presumption to meet legal requirements for a signature.[20]
- Equivalents to sections 11 and 12 of the Australian Electronic Transactions Act 1999, which deal respectively with requirements to produce and to retain documents, have been included in clauses 25–31 of the Bill. These sections were in turn based on articles 8 and 10 of the Model Law, although section 11 is a modified version of article 8, which related to requirements to present or retain *original* documents.[21] The drafters of the Australian legislation preferred to extend the scope of section 11 to requirements to produce any documents, not just originals, partly because Australian federal legislation does not specifically impose any requirements in respect of original documents. In ECom 2 we recommended that New Zealand adopt the same approach as Australia in applying the Bill to all requirements to produce documents. However given that New Zealand legislation does contain specific requirements

[20] See further, chapter 8, para 104.

[21] Emphasis added. See ECom 2, para 132.

in relation to original documents,[22] clause 32 of the Bill provides that a requirement to compare a document with an original may be met by comparing that document with an electronic form of the original.

- Equivalents to article 15 of the Model Law on Electronic Commerce (time and place of despatch and receipt of data messages) have been included in the Bill through the default rules appearing in clauses 9–13 of the Bill.
- The New Zealand Bill follows a similar structure to that of the Australian Act.
- The recommendation concerning potential liability of Internet Service Providers made in paragraph 333 of ECom 2 has not been dealt with in the Bill. Following further consultation with interested parties, the Ministry of Economic Development decided that the issue of ISP liability was so significant that separate legislation may be required.

14 In relation to the recommendations made in paragraphs 334–337 of ECom 2:

- The recommendations made in paragraphs 334 and 335 will await enactment of the proposed Evidence Code to which reference was made in the Introduction to this report.[23]
- The articles of the Model Law on Electronic Commerce which we recommended not be included in the Bill[24] have not been included. We have come to the view that it is unnecessary to enact an equivalent to article 13 of the Model Law and a brief discussion on that point is to be found in chapter 9 of this report.[25] In chapter 8 we confirm our recommendation that articles 16 and 17 of the Model Law (dealing with transportation documents) not be enacted.

---

[22] For examples see ECom 2, paras 123–125.

[23] See para 4.

[24] ECom 2, para 336.

[25] See paras 124–125.

Policy changes

15 In paragraph 9 we noted one important difference between the Electronic Transactions Bill and the recommendations made in ECom 2, that is that the Bill was intended to apply to all electronic transactions and communications unless specifically exempted rather than to electronic transactions conducted "in trade" as recommended in ECom 2.[26] The Bill will also apply, generally, to consumer transactions, although there are exceptions set out in part 2 of the Schedule to the Bill in relation to provisions of the Credit Contracts Act 1981 and the Credit (Repossession) Act 1997 (among others).

16 As there has been a different approach to the transactions to be caught by the Electronic Transactions Act it may be helpful to refer briefly to provisions of the Bill which outline its scope.

- Firstly, clause 14(1) of the Bill provides that part 3 of the Bill (dealing with the application of legal requirements to electronic transactions) applies to every enactment that is part of the law of New Zealand, whether passed before or after commencement of the Electronic Transactions Act. Thus, the Electronic Transactions Bill, when passed, will be an overarching statute. In this respect its function is comparable to that of the Interpretation Act 1999.
- Secondly, clause 14(2) excludes the application of part 3 to any enactment requiring information to be recorded, given, produced or retained, or requiring a signature to be given, or requiring a signature or seal to be witnessed in accordance with a *particular* electronic technology or on a *particular* kind of data storage device or by means of a particular kind of electronic communication (emphasis added). In addition, the application of part 3 of the Bill is excluded in respect of provisions of enactments specified in parts 1–4 of the Schedule, except to the extent that rules or guidelines issued with the authority of a court or tribunal specified in part 4 of the Schedule provide otherwise.[27] Provision has been made in clause 14(3) of the

---

[26] ECom 2, para 337.

[27] Clauses 14(2)(b)–(e).

Bill for the Schedule to be amended, repealed or substituted by Order in Council. As the terms of the Electronic Transactions Bill introduced into Parliament are set out in appendix A we do not refer extensively to the enactments excluded.

- Thirdly, although a legal requirement[28] may be met through the use of electronic technology regarded as a functional equivalent of the paper-based requirement, nothing in part 3 of the Bill requires anyone to use, provide or accept information in electronic form without that person's consent: see clause 16(1). For the purposes of part 3 of the Bill a person may consent to use, provide or accept information[29] in an electronic form subject to conditions regarding the form of the information or the means by which the information is produced, sent, received, processed, stored or displayed; and consent may be inferred from the conduct of a person: see clause 16(2). Clause 16(3) provides that both 16(1) and (2) are for the avoidance of doubt. We note that we recommended in ECom 2[30] that in relation to the delivery or service of notices and other documents in certain consumer transactions, electronic delivery or service should be effective only where there was consent.[31] If clause 16(2) is enacted in its current form, consent can be express or inferred from conduct.

17 Another policy change has been in relation to the definition of the term "writing" which was introduced by section 29 of the Interpretation Act 1999. In paragraph 28 of ECom 2 we expressed the view that electronically generated messages would, from 1 November 1999, qualify as "writing" as a result of the enactment of that provision. In its present form, section 29 provides that the term "writing":

---

[28] The term "legal requirement" is defined in clause 15(2) to mean a requirement in an enactment to which part 3 of the Bill applies and which is referred to in subpart 2 of part 3 and "requirement" includes an enactment that imposes consequences if it is not met or, if met, leads to a special permission or other result.

[29] "Information" is defined in clause 5 to include "information (whether in its original form or otherwise) that is in the form of a document, a signature, a seal, data, text, images, sound, or speech".

[30] ECom 2, para 340, 4th point.

[31] See also ECom 2, paras 88–89, 93 and 110.

Includes representing or reproducing words, figures, or symbols –

(a) In a visible and tangible form by any means and in any medium:

(b) In a visible form in any medium by electronic means that enables them to be stored in permanent form and be retrieved and read.

Clause 36 of the Bill will substitute an amended definition of the term "writing" in the Interpretation Act 1999. In its amended form the definition would be:

"Writing" means representing or reproducing words, figures, or symbols in a visible and tangible form by any means and in any medium (for example, in print).

18 A more restricted definition of the term "writing" in the Interpretation Act 1999 has been favoured by the Ministry of Justice because, although the provisions of clauses 18–21 of the Electronic Transactions Bill will enable certain legal requirements for writing to be fulfilled by electronic means, there will be statutory exclusions from that regime. If the definition of the term "writing" in section 29 of the Interpretation 1999 remained unamended after passage of the Electronic Transactions Bill then unintended consequences could result, namely:

- the safeguard in the Bill with respect to consent to use of electronic technology would be circumvented; and
- legal requirements excluded from the scope of the Electronic Transactions Bill might be capable of being met using such technology.

Miscellaneous provisions

19 Nothing in part 3 of the Electronic Transactions Bill affects any legal requirement to the extent that the requirement relates to the content of information: see clause 33.

20 Clause 31 of the Bill maintains that copyright in a work is not infringed by the generation of an electronic form of a document or the production of information by means of an electronic communication if they are carried out for the purposes of meeting a legal requirement by electronic means. A similar provision is contained in sections 11(6) and 12(6) of the Electronic Transactions Act 1999 (Cth).

21 The Governor-General may, by Order in Council, make regulations prescribing conditions that must be complied with in order to meet by electronic means legal requirements specified in those regulations by electronic means: see clause 35 of the Bill.

22 The Act will come into force on a date to be appointed by the Governor-General by Order in Council, as stated in clause 2 of the Electronic Transactions Bill.

3
Conflict of laws

23 THE ISSUE OF CONFLICT OF LAWS arises when parties to a dispute have connections with more than one country.[32] Four broad issues arise in the New Zealand context:[33]

- whether a New Zealand court has jurisdiction to hear a dispute; and, if so
- whether the New Zealand court will exercise that jurisdiction, or leave the dispute to be resolved by the courts of another country;
- which country's law will be applied by the court exercising jurisdiction – the issue of "choice of law"; and
- whether a foreign judgment can be enforced in the New Zealand courts, or equally whether a judgment of a New Zealand court can be enforced in another country.

24 Different countries apply different rules when determining these issues of jurisdiction, choice of law and enforcement of judgments. The increasing importance of electronic commerce challenges our existing conflict of laws rules, because of:

- the difficulty in applying traditional tests grounded on the geographic location of something that was done (for instance, where a contract was entered into, where services were performed or where goods were delivered) in an electronic environment; and
- the greater volume and frequency of cross-border transactions generated through the use of electronic means of communication.[34]

---

[32] See further *Laws NZ: Conflict of Laws: Jurisdiction and Foreign Judgments*, para 1.

[33] See ECom 1, para 254 and ECom 2, para 271.

[34] See ECom 2, paras 273–275.

The uncertainty of rules which will apply to determine questions of jurisdiction, choice of law and enforcement of judgments when international transactions are involved, continues to be a barrier to international trade for New Zealand parties.

Hague Convention

25 In ECom 2 we discussed work being undertaken at the Hague Conference on Private International Law to negotiate an international convention on jurisdiction and judgments in civil and commercial matters. While we had hoped to consider in detail the content of the draft Convention in this report, progress on the draft has not been as rapid as initially planned by the Hague Conference. Although a preliminary draft convention has been prepared,[35] concerns about that draft on the part of the United States and some other participants have led to a decision to defer the Diplomatic Conference previously scheduled for October 2000. We do not now expect this important work to be completed until early 2002.

26 Despite other disagreements relating to this project, it has been recognised that the draft convention will need to deal adequately with electronic commerce issues. A separate meeting to identify electronic commerce issues raised by the project was held in Ottawa in March 2000, and a further meeting to discuss those electronic commerce issues will take place in February 2001, again in Ottawa. New Zealand has been, and will continue to be, represented at all major meetings of the Hague Conference dealing with these issues by Mr David Goddard.

Co-ordination with Australia

27 In September 2000 the Minister for Trade Negotiations and his Australian counterpart signed a Memorandum of Understanding on Business Law Co-ordination between Australia and New Zealand. The Memorandum of Understanding identifies possible areas for furthering the co-ordination of business laws and regulatory practices between the two countries. The Memorandum should permit Australia and New Zealand to achieve a greater degree of co-ordination at a regional level which will, in turn,

---

[35] This draft can be viewed on the Hague Conference website, <http://www.hcch.net>.

provide the business community with greater predictability regarding the law and forum for disputes. Regional initiatives such as the Memorandum of Understanding between Australia and New Zealand are likely to progress at a much faster pace than multilateral arrangements such as those being negotiated at the Hague Conference on Private International Law.

Applicable law

28 There are fewer successful conventions dealing with issues of applicable law in cross-border commercial transactions than in relation to questions of jurisdiction and enforcement of judgments, and these issues are of real concern to businesses engaged in electronic commerce. Uncertainty as to the applicable law governing contracts or other types of liability may act as a barrier to electronic commerce. It is not unusual for a New Zealand court to have jurisdiction to hear a dispute, but to apply the law of another country in determining a particular issue or issues.[36]

29 There are three situations in which issues as to applicable law will arise:

- Contractual disputes, where the contract contains a clause specifying the applicable law. Different countries take different approaches in relation to such clauses. The clause may be wholly ineffective, or domestic law may be applied in relation to certain issues (for example, consumer protection or employment) despite a choice of foreign law. But in most cases, in most countries, such clauses will be given effect. Parties should be encouraged to address specifically questions of choice of law in contractual documents although, it must be noted, the courts will not always give effect to the parties' choice.[37] Difficulties in dealing with questions of forum can be resolved more readily where arbitration has been selected as the dispute resolution

---

[36] *Laws NZ*, above n 32, para 1.

[37] In *Jardine Risk Consultants Limited v Beal* (29 June 2000) unreported, Court of Appeal, CA 208/99, the Court of Appeal had to consider whether the choice of law clause in an employment contract had been impliedly varied. See also *Bilgola Enterprises Ltd & Ors v Dymocks Franchise Systems (NSW) Pty Ltd* [2000] 3 NZLR 169 (CA) as an example of a case where the High Court judgment was reversed because of the way in which the High Court approached the question of foreign law.

process; in that regard, it is noted that the Convention on the Recognition and Enforcement of Foreign Arbitral Awards (the New York Convention)[38] more readily permits cross-border enforcement of arbitral awards than the current law governing cross-border recognition of judgments given by courts of competent jurisdiction.

- Contractual disputes, where the contract is silent as to the applicable law. In these cases the forum hearing the dispute will apply its domestic rules of public international law to ascertain the applicable law. There is real uncertainty under the law of New Zealand and many other countries as to the rules that should be applied.
- Non-contractual disputes. There is also uncertainty about what law will be applied in these situations, where the parties have not had the opportunity to select the applicable law.

30 Uncertainty as to applicable law will not be resolved in the short term. The Commission is of the view that it would be desirable for an international body to consider what principles should be applied in determining what the applicable law should be in cross-border commercial transactions and, in addition, the circumstances in which agreement as to applicable law will be given effect. The Commission recommends that representations be made to the Hague Conference on Private International Law to undertake that task.

---

[38] In force in New Zealand by virtue of s 5(f) of the Arbitration Act 1996; the Convention is set out in the Third Schedule to that Act.

4
Criminal law

NEW ZEALAND LEGISLATION

31 THE ISSUE OF CRIMINAL LIABILITY for offences involving computers was discussed in *Computer Misuse*[39] and ECom 2.[40] In the former report the Commission recommended that four new offences covering a range of computer-based offending be created. These recommendations were intended to add to those made in *Dishonestly Procuring Valuable Benefits*,[41] which proposed a reform to close the gap in the law exposed by the Court of Appeal in *R v Wilkinson*.[42] In ECom 2 the Commission proposed an additional offence be created: of intentionally and without authority gaining access to a computer system.[43] This offence was proposed to cover the situation where a hacker intentionally accesses a computer system without intending to obtain a benefit or cause a loss. Even if a hacker does nothing while in the system, such activity has the potential to cause considerable financial loss; for example the owner or manager of the system will incur costs if the system has to be checked to determine whether there has been any damage.[44]

32 There is currently before Parliament the Crimes Amendment Bill (No 6) which contains offences aimed at computer-based offending. A Supplementary Order Paper[45] to that Bill implements the

---

[39] Law Commission *Computer Misuse: NZLC R54* (Wellington, 1999).

[40] See chapter 12, paras 180–196.

[41] Law Commission *Dishonestly Procuring Valuable Benefits: NZLC R51* (Wellington, 1998).

[42] [1999] 1 NZLR 403 (CA).

[43] ECom 2, para 187.

[44] ECom 2, para 192.

[45] No 85, introduced 7 November 2000.

Commission's recommendation by providing (in addition to the provisions of the original Bill) for an "access only" offence, punishable by up to two years imprisonment. While the Commission originally proposed a greater maximum penalty of three years imprisonment,[46] we are nevertheless satisfied that these measures should afford a greater level of protection against the misappropriation of electronic information. Creation of such offences should make it easier for plaintiffs in civil proceedings to pursue causes of action,[47] as courts have historically evidenced a desire, when developing the common law and equity, to take account of policy changes distilled from statute.[48]

INTERNATIONAL INITIATIVES

33 In domestic law, the criminal law provides a solid base on top of which the civil law can operate, safe in the knowledge that criminal sanctions are available in cases of extreme conduct. The Electronic Transactions Bill (based on the UNCITRAL Model Law on Electronic Commerce, which has been adopted in various forms in other jurisdictions – see appendix D) establishes the domestic and international civil law, and the Crimes Amendment Bill (No 6) offences will provide domestic criminal sanctions. However there is no underlying international criminal regime to handle cross-border cases of computer hacking and other offences.[49]

---

46 ECom 2, para 192.

47 Possible causes of action for computer misuse include breach of confidence, unlawful interference with economic relations, and unjust enrichment. These actions are discussed more fully in chapter 7.

48 See ECom 2, paras 211–227. See also the observation of Lord Diplock in *Erven Warnink BV v J Townend & Sons* [1979] AC 731, 743 that "[w]here over a period of years there can be discerned a steady trend in legislation which reflects the view of successive Parliaments as to what the public interest demands in a particular field of law, development of the common law in that part of the same field which has been left to it ought to proceed on a parallel rather than a diverging course".

49 This issue was explored in a paper "An International Approach to Computer Crime" given by Paul Heath QC to the Commercial Law Association seminar UNCITRAL and the Developing International Law of Electronic Commerce (New York, 24 February 2000), published Documentary Credit World 34 (June 2000, Vol 4 No 6); also available on the Commission's website under "Speeches".

34 Regarding the importance of international co-operation in controlling the increase in global fraud, we note that the Director of the Serious Fraud Office has observed that while mutual legislation is important, direct contacts with equivalent agencies overseas are more helpful in obtaining timely and meaningful assistance.[50] Similarly, reciprocal procedures for extraditing offenders are important. We must also ensure that the territoriality or scope of our criminal law is sufficient to apply to actions by offenders located in New Zealand affecting overseas networks, and vice versa (applying to actions by offenders located overseas which affect New Zealand networks).

35 Two current international initiatives which aim to address the need for an international criminal regime are described below.

United Nations

36 The Tenth Congress on the Prevention of Crime and the Treatment of Offenders was held in Vienna on 10–17 April 2000 and representatives of the New Zealand Government were present. A workshop on Crimes Related to the Computer Network concluded that:[51]

- computer-related crime should be criminalised;
- adequate procedural laws were needed for the investigation and prosecution of cyber-criminals;
- government and industry should work together towards the common goal of combating and preventing computer crime so as to make the internet a secure environment;
- improved international co-operation is needed in order to trace criminals on the internet;
- the United Nations should take further action with regard to the provision of technical co-operation and assistance concerning crime related to computer networks.

---

[50] Serious Fraud Office Annual Report to 30 June 1999 (quoted in 22 TCLR 47/3).

[51] United Nations Congress, *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, A/CONF.187/L.10, report of Committee II (Workshop on Crimes Related to the Computer Network), Vienna, April 2000.

Council of Europe and other States

37 The Council of Europe is based in Strasbourg, France, and has 41 member states. It has released a draft Convention on Cyber Crime, which was debated recently in meetings at the White House and among representatives of the Group of Eight industrialised countries in Berlin.[52] Because of the international interest in the draft Convention, non-member states (including Canada, Japan, South Africa and the United States) are participating in these negotiations.

38 The draft provides for the co-ordinated criminalisation of computer hacking and hacking devices, illegal interception of data and interference with computer systems, computer-related fraud and forgery. It also prohibits online child pornography, as well as the reproduction and distribution of copyright material.

Conclusion

39 The Commission supports New Zealand's continued involvement in international work on computer crime issues. On the domestic front, the Commission favours an approach to domestic criminal law affecting computer misuse which is compatible with the approach taken by major trading partners. The Commission is likely to be making submissions to the Select Committee on the Crimes Amendment Bill (No 6) when the Select Committee considers the Supplementary Order Paper.[53] The Commission recommends that the Ministry of Justice and the Ministry of Foreign Affairs and Trade continue to monitor the international initiatives described in this chapter.

---

[52] See "Cyber crime treaty raises concern" *The Dominion*, Wellington, New Zealand, 30 October 2000, 5. Version 22 of the draft Convention can be downloaded from <www.conventions.coe.int/treaty/EN/cadreprojets.htm> (last accessed 1 November 2000).

[53] Parliament resolved on 16 November to refer the Supplementary Order Paper to the Law and Order Select Committee.

5
Privacy

40 In our previous report, ECom 2, we noted that the immense speed, power, accessibility and storage capacity of the internet poses a new and unique danger to information privacy.[54] The privacy of personal information stored in paper-based systems is protected by the cost and inconvenience of retrieval, the impermanence of the forms in which the information is stored, the incompatibility of collections with available indexes, and the effective undiscoverability of most of the data. These logistical difficulties in accessing information that have the effect of constraining the use or disclosure of data disappear on the internet where the user generates a data trail of personal information that may be relatively easily retrieved and matched. This lack of information privacy is of concern to potential consumers and represents an obstacle to electronic commence. Many consumers are unwilling to use the internet to buy goods and services if the security of their personal information cannot be guaranteed.

41 In New Zealand, the Privacy Act 1993 provides a high level of protection for the personal information of New Zealand consumers dealing with companies based in New Zealand.[55] The Act is technologically neutral and applies to the electronic commerce sector as well as the paper-based environment. The Commission concluded, in its earlier report, that the Act provides sufficient protection to ensure that New Zealand consumers are not dissuaded from dealing with New Zealand businesses engaged in electronic commerce on account of concerns over the privacy of their personal information.[56] However, we drew attention to the fact that the

[54] ECom 2, para 165.

[55] Note that the protection afforded by the Privacy Act 1993 is for individual (living natural persons) only: see the long title and s 2.

[56] ECom 2, para 177.

Privacy Act 1993 may not offer sufficient safeguards for the personal information of non-New Zealand consumers.[57] This is of concern because it potentially has a detrimental effect on the ability of New Zealand companies to do business with consumers in overseas countries.

European Union Directive

42 The effect of inadequate privacy protection on our international trade is of particular concern with regard to the European Union (EU). Privacy law in the EU is regulated by the Directive of the European Parliament and Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data. This Directive establishes a high level of protection for the privacy of personal data within the EU, and requires member states to ensure that the transfer of personal data to a non-EU country may only take place if a continued "adequate" level of privacy protection is guaranteed.[58]

43 The Privacy Act 1993 is, in general, sufficiently robust to meet most of the criteria of the European Directive for the transfer of personal data to a third country. However, two factors that could prevent the Act from being deemed "adequate" under the European Directive were identified in the review of the Privacy Act undertaken by the Privacy Commissioner[59] and noted in ECom 2.

- First, section 34 of the Act provides that certain requests in relation to personal information held by an agency may only be made where the requestor is either a New Zealand citizen, a permanent resident of New Zealand or is in New Zealand at the time.
- Second, there is no statutory constraint on the export or re-export of personal data information from New Zealand to countries that do not have an adequate privacy regime.

---

[57] ECom 2, paras 174–177.

[58] Article 25 of the Directive of the European Parliament and Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data.

[59] Office of the Privacy Commissioner *Necessary and Desirable: Privacy Act 1993 Review: Report of the Privacy Commissioner* (Wellington, 1998). We rely heavily on the Privacy Commissioner's analysis in this discussion.

44 The Privacy Commissioner's two proposals to address these matters were discussed in ECom 2.[60] The first would extend the right of access in section 34 to non-New Zealanders who are not present in New Zealand at the time the request is made. The second would amend the Act to prevent the diversion of data transmissions through New Zealand to third countries with inadequate protection for personal information. Submissions supported these recommendations. The Associate Minister of Justice has agreed that the Privacy Act be amended to give effect to these two proposals and is considering the inclusion of amendments in a suitable legislative vehicle.

Caching

45 ECom 2 raised one substantive matter for comment: the application of the Privacy Act 1993 to the process of caching. Caching occurs when a webpage accessed by a user is temporarily stored by the user's computer (client caching) or by the network server that provides the user with internet access (proxy caching). When a webpage is requested, the client computer or network server first checks whether it holds a copy of the requested page. If it does, it will display the cached version to the requester rather than accessing the page via the internet. Caching is used because it enables faster access to information on the internet and reduces costs.

46 Client caching would generally be excluded from the ambit of the Privacy Act 1993. The effect of section 56 is that individuals are not required to comply with the Act if they collect or hold information solely or principally for the purposes of, or in connection with, that individual's personal, family or household affairs. However, proxy caching may come within the ambit of the Act and thus have to comply with the principles of the Act set out in section 6. The Commission sought submissions in relation to the privacy issues raised by caching, and particularly as to:

- whether there are any practical problems or issues in the application of the existing law;
- whether those problems arise in relation to collecting, holding or giving access to information; and
- if a law change is warranted, how that might be framed.

---

[60] ECom 2, para 274, recommendations 35(a) and 61.

47 Three submissions were received on the subject of caching. None of the submission makers were aware of any *practical* problems or issues in the application of the existing law. However, one submitter[61] thought that a *theoretical* argument could be made that caching gave rise to privacy compliance issues in relation to the collection of, holding of, and giving access to, personal information. Because caching enables efficient and cost-effective use of the internet, the submitter suggested that legislation be enacted to provide that the technique of caching for the purposes of operating a computer system or network does not breach section 6 of the Privacy Act 1993.

48 The Privacy Commissioner did not think that such legislation was necessary or desirable. No caching issues had been brought to the attention of the Commissioner in complaints, enquiries or by any other means. The Commissioner agreed it would be problematic for ISPs if data privacy principles applied to information that is cached for purely technical reasons, but thought that such a problem, if it exists, would be best addressed through the interpretation of current data protection law; for example, by not treating personal data in ISP caches as being "readily retrievable". The Commissioner also thought that while caching currently poses no privacy problems, it is potentially problematic; for example, if it were to be used for profiling purposes. The Commissioner noted that no other country has such an exemption in its data protection laws.

49 The Law Commission agrees with the Privacy Commissioner. On our analysis of the Privacy Act 1993, any form of caching that occurs for purely technical reasons would not breach the principles in the Act. However, the use of such data for other purposes may fall within information privacy principles, depending on the purpose. The legal and technical experts we consulted support this position. Certainly, there are as yet no particular business compliance difficulties that would justify any kind of exemption. Accordingly, we are of the view that no law changes are needed to deal with this issue.

Cookies

50 A new issue was raised in one of the submissions:[62] the use of cookies. Cookies are small pieces of code that some web sites place on the computer hard drives of those who visit the website. The

---

[61] Submission from IT Law, Auckland, dated 30 June 2000.

[62] Above n 61.

cookie collects header information[63] about the visitor and may record click-stream data[64] as the visitor travels through the website. If the visitor is asked to supply information,[65] the cookie may record this also. A unique code may be assigned to each visitor and stored on the cookie. That cookie is then used to spot the visitor on any subsequent visit. Cookies are beneficial in that they facilitate user–server interaction and provide servers with the ability to monitor the use of their websites. However, they may also have a detrimental effect on the privacy of users. IT Law recommended that the proposed Electronic Transactions Act should contain a provision making it an offence to use cookies for the purpose of collecting, holding or giving access to personal information unless the website has indicated that such information will be gathered.

51 The Law Commission considers that the Privacy Act 1993, which would apply to the use of cookies within New Zealand, offers sufficient protection. Making the misuse of cookies a separate offence would be out of step with the regime established by that Act. The Privacy Commissioner, whom we consulted on this issue, does not support the creation of such an offence.

International harmonisation of privacy and data protection law

52 The privacy laws of different jurisdictions vary considerably. As noted above, the European Union has very strict data protection laws. The United States, in contrast, has predominantly relied on self-regulation.

53 Attempts have been, and are being, made at an international level to achieve a harmonious approach to privacy law. The impetus for this movement is the recognition that privacy is an important trade issue, as data privacy concerns can create a barrier to international

---

[63] This information can include: the user's internet protocol address; basic information about the browser, operating system and hardware platform of the user; the time and date of the visit; the Uniform Resource Locator of the webpage which was viewed immediately prior to accessing the current page; if a search engine was used to find the site, the entire query may be passed on; and depending on the browser, the user's e-mail address.

[64] Such as the pages visited, the time spent on each page and information sent and received.

[65] Such information is often requested by a commercial site to enable a user to register, subscribe, join a discussion group, enter a contest or complete a transaction.

trade. Because of this, the General Agreement on Trade in Services, for example, contains a term stating that the Agreement does not prevent member states from adopting measures necessary to secure "the protection of the privacy of individual records and accounts".[66]

54 In 1980 the Organisation for Economic Cooperation and Development (OECD) released the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, perhaps the most significant attempt at international harmonisation. The Guidelines were intended to provide a common framework for national privacy laws, in order to ensure that privacy concerns do not impose a barrier to international trade. The Guidelines establish technologically neutral principles for the collection, retention and use of personal information. The OECD's work in this area is ongoing. In 1998 it held a Conference on Electronic Commerce, which issued a Declaration reaffirming the objectives set out in the 1980 Guidelines. In December 1999 the OECD released its Consumer Protection Guidelines for E-Commerce, which also recommended compliance with the 1980 OECD privacy principles.

55 The OECD has created a Privacy Statement Generator to help implement the 1980 Guidelines in the electronic world. The Generator is intended to offer guidance on compliance with the Guidelines and to help organisations develop privacy policies and statements for display on their websites. The Generator uses a questionnaire to gather information about an organisation's personal data practices. The answers are then fed into a pre-formatted draft policy statement. The draft statement will provide an indication of the extent to which an organisation's privacy practices are consistent with the OECD Privacy Guidelines. The Generator offers links to private sector organisations with expertise on developing privacy policies, and to government agencies, non-governmental organisations and private bodies that give information on applicable regulations. The Generator has been endorsed by the OECD's 29 member countries and is available free of charge.[67]

---

[66] Article XIV(c)(ii), Part II, General Agreement on Trade in Services.

[67] The Generator may be found at <http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm>.

56 Other international agreements aimed at harmonising approaches to data privacy tend to resemble or reflect the OECD Guidelines. These include the United Nations Guidelines for the Regulation of Computerised Personal Data Files,[68] the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data,[69] and the EU Privacy Directive.[70] These agreements typically contain provisions permitting cross-border data flow to countries with similar levels of data protection.

57 There are also numerous international conferences and discussion forums which play an important role in contributing to international harmonisation through information exchange, education, and the development of instruments for privacy protection. These include annual international conferences of data protection commissioners, conferences of EU data protection commissioners, the International Working Group on Data

---

[68] United Nations High Commission for Human Rights Guidelines for the Regulation of Computerised Personal Data Files (Resolution 45/95 of 14 December 1990) were adopted by the UN General Assemble pursuant to article 10 of the UN Charter. The UN Guidelines apply to computerised personal data files (both public and private) and may be extended to manual files and to files on legal persons. Part A of the Guidelines are intended as the minimum privacy guarantees that should be provided in national legislation, and broadly reflect the basic principles in the OECD Guidelines. In addition, the UN Guidelines restrict the compilation of "sensitive data" within the principle of non-discrimination. UN members must take the United Nations Guidelines into account when implementing national regulations concerning computerised personal data files, but the procedures for implementing those regulations are left to the initiative of each State.

[69] The Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data asserts basic data privacy principles that are similar to those in the OECD Guidelines. However, it also includes a principle requiring appropriate safeguards for special categories of data (sensitive data) that reveal racial origin, political opinions or religious or other beliefs, that concern health or sexual life, or that relate to criminal convictions (article 6). The Convention is open to the accession of any State, whether a member of the Council of Europe or not.

[70] The information privacy principles of the EU Directive are framed in terms of processing personal data but are in general terms similar to the information privacy principles found in the OECD Guidelines and the Council of Europe Convention. In several respects the principles of the Directive offer greater protection to data privacy. The EU Directive is likely to prove hugely influential outside the EU because of the data flow controls that it instigates.

Protection in Telecommunications, the International Organisation for Standardisation,[71] and the International Chamber of Commerce.

58 On another level, mechanisms have been developed to implement and enforce privacy principles on global networks. These include the development of means whereby consumers may use the internet anonymously (for example, the use of anonymous payment systems and digital certificates to avoid the need for personal data disclosure), the development of software that enables the user to control the use of cookies, the creation of industry standards and the certification of adequate privacy practices by trusted third parties.

59 New Zealand is highly dependent on its ability to trade internationally. For the last 16 years our governments have shown a commitment to reducing barriers to international trade. The international harmonisation of privacy and data protection law is an important factor in achieving that goal. We recommend continued involvement by New Zealand in these international forums.

---

[71] The ISO Ad Hoc Advisory Group on Privacy undertook a study to examine whether there is a need, under the pressure of technological advances in global information structures, for an international standard to address information privacy, measure privacy protection and ensure global harmonisation. In June 1988 the Advisory Group concluded that it was premature to reach a determination on the desirability and practicality of ISO undertaking the development of international standards relevant to the protection of personal privacy.

6
Banking

60 In ECom 2 the Commission requested submissions regarding the issue of liability for unauthorised electronic banking transactions.[72] We queried whether the risk of unauthorised transactions is appropriately allocated between financial institutions and their customers. If reform were desirable, we queried whether this should take the form of legislation, or an amendment to the current self-regulatory Code of Banking Practice.[73]

Submissions

61 The nature of the submissions received on these issues reflected the nature of the parties represented by the submitters. For example:

- the Bankers' Association considered that the current allocation of liability was appropriate, and that in practice the banks bore the burden of proving that a customer had contributed to or caused a loss, even if the Code did not expressly state this;[74]
- the Ministry of Consumer Affairs considered that the onus of proof should lie with the card issuer, and that allocation rules should be clear, simple and decisive. The Ministry noted that the Code placed a higher burden on the customer than, for

---

[72] ECom 2, chapter 15. By way of background, chapter 10 of the Office of the Banking Ombudman's Annual Report 1996–1997 discusses some of the disputes that have arisen regarding the allocation of liability between customers and banks, and how the Code of Banking Practice has been interpreted by the Office in those situations.

[73] The relevant extracts from the Code of Banking Practice are reproduced in appendix 4. We note that the member banks of the New Zealand Bankers' Association have agreed to comply with the Code, however those card issuers which do not belong to the Bankers Association may be bound by the Code's predecessor, the EFT Code of Practice. See ECom 2, para 305.

[74] Submission of New Zealand Bankers' Association, dated 6 July 2000.

example, Good Banking (the United Kingdom Code), and that if electronic banking systems were more secure then unauthorised transactions would be easier to identify;[75]

- the Commercial and Business Law Committee of the New Zealand Law Society also considered that card issuers had a responsibility to establish approved systems, although it noted that in general a card holder is best placed to protect their card from loss or theft and their PIN (Personal Identification Number) from compromise, and concluded that liability should be allocated to the party in the best position to manage the exposure.[76]

Banking Ombudsman

62 The role of the Banking Ombudsman is that of independent and impartial arbitrator of disputes over the provision of banking services. In the 1998–1999 Annual Report, the Banking Ombudsman noted that complaints about cards (both debit and credit) had increased by 57 per cent, and that cases actually taken up for investigation had more than doubled.[77] These increases reflected the difficulty in assessing whether the bank or customer (or both) should bear liability for the loss when a card has been used to make fraudulent withdrawals.[78] The Banking Ombudsman expressed the view that the rules set out in the current Code of Banking Practice were not always easy to interpret, and that the terms and conditions on which banks issued cards were not always consistent with these rules.[79]

63 The Banking Ombudsman noted that the degree of consumer protection is comparatively low by international standards, as the Code allows banks to require their customers to meet a high standard of PIN and card protection.[80]

---

[75] Submission of the Ministry of Consumer Affairs, dated 17 July 2000.

[76] Submission of the Commercial and Business Law Committee of the New Zealand Law Society, dated 19 July 2000.

[77] Banking Ombudsman Annual Report 1998–1999, 8. Cases not taken up may have been referred elsewhere, the Banking Ombudsman may have declined jurisdiction, or the complaint may have been withdrawn or abandoned.

[78] Above n 77, 8.

[79] Above n 77, 8.

[80] Banking Ombudsman Annual Report Case Note Compendium, 11. See also ECom 2, paras 306–307.

Australia

64 In ECom 2 we discussed the proposals of the Australian Securities and Investment Commission (ASIC) EFT (Electronic Funds Transfer) Working Group for an expanded EFT Code of Conduct.[81] In our view, it is helpful to consider the Australian approach to risk allocation in electronic banking, given the trans-Tasman flow of persons (many of whom may hold bank accounts in both countries) and the fact that four of the five largest retail banks in New Zealand are subsidiaries of Australian banks.

65 Since ECom 2 was published, the ASIC Working Group has released a second draft for an expanded EFT Code of Conduct.[82] Part A of that draft proposes three options for allocating liability for unauthorised transactions:[83]

- Option A – substantially retaining the approach of the current Code;
- Option B – apportioning liability between the user and account institution on a no-fault basis, unless the institution can prove that the user was fraudulent or grossly negligent in a specific request;
- Option C – the United States approach, where the user is only liable for delays in reporting lost or stolen devices or failing to report unauthorised transactions shown on a periodic statement.

66 The Working Group, after consultation, declared majority support for Option B. However, the Code has not yet been finalised as ASIC awaits the introduction of the (Australian) Financial Services Reform Bill, as ASIC wishes to ensure that the proposed EFT Code is not inconsistent with this legislation.

Conclusion

67 The Commission finds persuasive the views and experiences of the independent Banking Ombudsman in relation to the problems said to be caused by the current Code of Banking Practice. However, the Commission is convinced that it is inappropriate, at this time, to legislate for the allocation of risk in unauthorised transactions, because:

---

81 ECom 2, para 311.

82 Published January 2000; available at <www.asic.gov.au>.

83 Above n 82, 16.

- we believe it is better to leave these issues to regulation by Code; and
- it is more appropriate to deal with the problems which have been identified to date in the forthcoming review of the Code. We note, in that regard, that a clarification of the provisions of the Code of Banking Practice was favoured by the majority of submitters.

68 By November 2001 the Code of Banking Practice will have been operative for five years. The Banking Ombudsman notes that the existing allocation of risk in the Code was undertaken soon after credit cards were introduced.[84] For that reason, the forthcoming review of the Code of Banking Practice by the Bankers' Association (which should take account of the views of the Banking Ombudsman and the Ministry of Consumer Affairs) seems to be the most appropriate forum in which to review these issues.

69 Accordingly, we recommend that the Bankers' Association, in conducting the review of the Code of Banking Practice by November 2001, take into account the problems identified by the Banking Ombudsman, as well as Australian developments in consideration of amendment to the rules regarding liability for unauthorised transactions.

---

[84] Banking Ombudsman Annual Report Case Notes Compendium, 11.

7
The law of torts

70 In ECom 1 we discussed the application of the law of torts in the electronic environment and noted the potential breadth of liability for tortious acts.[85] We sought submissions on whether legislation should be introduced to limit the boundaries of liability in tort, having regard to the problems in defining one's neighbourhood in the electronic environment. The great majority of the submissions received supported our provisional view that it would not be feasible to introduce legislation because of the difficulty in articulating restrictions in a sensible and workable manner.

71 In ECom 2 we addressed two further issues: whether there were any significant gaps in the law's protection of information that has been wrongfully obtained,[86] and the need to clarify the basis of ISP liability for the acts and omissions of their subscribers.[87] The response to these issues, and our conclusions, are discussed below. We discuss, in particular, ISP liability for third party content that is defamatory or offensive.

THE PROTECTION OF INFORMATION THAT HAS BEEN WRONGFULLY OBTAINED

72 Most of the causes of action that may protect against wrongful use of information are of common law or equitable origin. The evolutionary nature of common law and equitable causes of action make them adaptable to new circumstances, but it is difficult to be certain that existing causes of action will provide a remedy until cases come before the courts. Our provisional view, in ECom 2, was that a need for legislative intervention to provide greater protection against the misuse of information had not, as yet, been

[85] ECom 2, paras 138–192.

[86] ECom 2, paras 201–239.

[87] ECom 2, paras 240–261.

demonstrated.[88] We suggested that the protections offered by the equitable action for breach of confidence, the tort of unlawful interference with economic relations, unjust enrichment and breaches of section 9 of the Fair Trading Act 1986 should be sufficient to deal with most cases. However, as there may be a demonstrable need in the near future for added protection, we sought submissions on whether the existing statutory, common law and equitable actions are sufficient to meet the needs of those involved in electronic commerce.

73 In addition, we asked what form any additional protection should take, specifically:

- should information be redefined as property; or
- should New Zealand codify the law of unjust enrichment; or
- should a statutory tort be introduced that would give the owner of a computer system a right of action against a person where that person had breached criminal legislation dealing with computer misuse and, as a result, caused loss or obtained a benefit?[89]

---

88 ECom 2, para 207.

89 Some overseas jurisdictions have legislated to create civil remedies based on computer crime statutes. In the United States, at a federal level, US Code 18 § 1030(g) states that "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief". Many US State jurisdictions have similar civil relief provisions as part of their computer crime law. For example, 720 ILSC 5/16D-3 (2000) (c) "Whoever suffers loss by reason of a violation of subsection (a)(4) of this Section [the section concerned with losses suffered by computer users] may, in a civil action against the violator, obtain appropriate relief. In a civil action under this Section, the court may award to the prevailing party reasonable attorney's fees and other litigation expenses"; RI Gen Laws § 11-52-6 (2000) (a), "[a]ny person injured as a result a violation of this chapter [chapter 52 – Computer Crime] may bring a civil action against the violator for compensatory damages, punitive damages, court costs, and such other relief as the court deems appropriate, including reasonable attorneys' fees"; Cal Penal Code § 502 (2000) (e)(1), "In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data may bring a civil action against any person convicted under this section for compensatory damages, including any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access."; Tex Civ Prac & Rem § 143.001 (2000) (a), "[a] person who is injured or whose property has been injured as a result of a violation under Chapter 33, Penal Code,

74 Only two of the submissions received addressed these issues. Both suggested that existing statutory, common law and equitable actions are not sufficient to meet the needs of those involved in electronic commerce. They supported our provisional view that it would be inappropriate to redefine information as property.[90] Neither commented on the proposal to codify the law of unjust enrichment. Both submissions showed a degree of support for the introduction of a statutory tort: one favoured a statutory tort covering a wide range of acts of computer misuse, while the other went only so far as to support further consideration being given to a statutory tort as set out in paragraph 67 of ECom 2. None of the submissions indicated that the New Zealand insurance market would not be able to provide adequate cover for businesses engaging in electronic commerce.[91]

75 We have reached the view that it would be undesirable to make recommendations in this difficult area of law while it is unclear precisely what problems will need to be addressed in the long term. We prefer the view that, at least in the meantime, the common law should be allowed to develop to meet changing circumstances.

CLARIFICATION OF ISP LIABILITY FOR THE ACTS AND OMISSIONS OF SUBSCRIBERS

76 In ECom 2 we recommended that the Electronic Transactions Act contain a provision providing that ISPs have no civil or criminal liability with respect to information generated by their subscribers unless:

- the ISP has actual knowledge of the existence of information on the website which would be actionable at civil law or constitute a criminal offence; and

---

[Computer Crimes] has a civil cause of action if the conduct constituting the violation was committed knowingly or intentionally." Note: US legislation cited and available on Lexis.

Of interest in New Zealand is that, as long ago as 1975, the Listening Devices Bill 1975 created a number of offences related to using a listening device to intercept private communications. Clause 25 created a statutory tort based on some of the offences in the bill. The Bill was not passed, being replaced by a similar bill, the Misuse of Drugs Amendment Bill 1978 (passed as the Crimes Amendment Bill in 1979), when there was a change of government. The new bill did not provide for a civil remedy.

90 See ECom 2, para 230 for the Law Commission's reasons for reaching this conclusion.

91 See ECom 2, paras 236–239.

- the ISP fails to remove promptly any offending information of which it has knowledge.

We also recommended the Act provide that an ISP should not be liable for any reposting of information by a third party unless it obtains actual knowledge of such a reposting and fails to act to remove the information.

77 We noted that these recommendations were consistent with the treatment of ISP liability by a number of states.

78 We received two submissions on the issue of clarification of ISP liability. Both supported the proposal that ISPs should not be liable with regard to information on a website provided by them unless they had actual knowledge of the information and failed to remove it promptly. The New Zealand Law Society Commercial and Business Law Committee noted that this proposal would still leave ISPs with the burden of making judgments on whether material that comes to their knowledge is unlawful or may lead to liability.

79 An argument may be made that the speed with which information may be disseminated via the internet and the great difficulty of regulating content constitute a sufficient distinction in media to justify treating ISPs differently from other non-electronic information providers. The US Congress has done just this with the Communications Decency Act 1996,[92] which effectively immunises providers of interactive computer services from civil liability in tort with respect to material disseminated by them but created by others, even where the provider has actual knowledge of the material. The breadth of this immunity has been criticised by commentators[93] and by the judiciary.[94] We are not persuaded that our recommendation would leave an unduly onerous burden on ISPs. Accordingly, we confirm our earlier recommendation.

---

[92] Communications Decency Act 1996, s 230. The provision was passed in response to the finding of liability in *Stratton Oakmont v Prodigy Services* 23 Media L Rep (BNA) 1794 (NY Sup Ct May 24, 1995); discussed ECom 2, para 249.

[93] BJ Waldman "A Unified Approach to Cyber-Libel: Defamation on the Internet, a Suggested Approach" (1999) 6 Rich J L & Tech 9, see <http://www.richmond.edu/jolt/v6i2/note1.html> (last accessed 29 November 2000).

[94] *Blumenthal v Drudge and America Online* (1998) 992 F Supp 44 (DDC).

Defamation

80 In ECom 2 we expressed the view that there was a need for ISPs to be protected through the innocent dissemination defence provided by section 21 of the Defamation Act 1992.[95] Section 21 protects distributors (and certain others) against liability for defamation provided that the distributor had no knowledge of the defamatory material and did not know that the matter distributed was likely to contain material of a defamatory nature, and that the lack of knowledge was not due to any negligence on the distributor's part. It is arguable whether an ISP would be deemed a distributor under the Act. Accordingly, we recommended that the definition of "distributor" in section 2(1) of the Act be amended to include explicit reference to an ISP and that ISPs be defined in a separate definition to include providers of the services discussed in paragraph 242 of the report. One submission was received on this issue, which supported the proposal. We reiterate this recommendation.

Offensive publications

81 Another area of potential ISP liability for the actions of third parties is the publication of offensive material. Sections 122–123 of the Films, Videos and Publications Classification Act 1993 create a number of offences in relation to objectionable and restricted publications. Some of these offences[96] would probably capture the actions of an ISP acting purely as an access provider.[97] This issue was not specifically addressed in ECom 2. However, in keeping with our position with regard to ISP liability for third party information, we consider that an ISP acting purely as an access provider should not be liable in relation to offensive material requested or posted by clients, unless the ISP had actual knowledge of the infringing publication.[98] In particular, we do not consider

---

[95] ECom 2, paras 262–270.

[96] See ss 123(1)(b) and (e), 125(1)(a), 127(1) and 131(1).

[97] This involves acting as a conduit for the information of others or hosting websites that contain the information of others. See ECom 2, paras 240–246 for a description of ISPs as pure access providers, content providers and mixed providers.

[98] The Law Commission made a submission on the Ministry of Economic Development's *Discussion Paper on Electronic Transactions Bill* to this effect.

that ISPs should be subject to the strict liability offences created by sections 123 and 125 or those offences where lack of knowledge is excluded as a defence. Liability under these sections would place a monitoring duty on ISPs that would be unduly onerous and costly, given the amount of material that would have to be screened.

82 Overseas jurisdictions have approached the issue of ISP liability for offensive internet content provided by third parties in a number of ways. Some of these approaches are discussed below.

Australia

83 The Australian Broadcasting Services Amendment (Online Services) Act 1999 provides a regulatory framework that places obligations on internet content hosts and service providers with regard to the prohibited content[99] of third parties. Very briefly, if the prohibited content is hosted in Australia, it must be removed and not hosted in the future, once a "take down" notice is issued by the Australian Broadcasting Authority (ABA). If the prohibited content is hosted outside Australia, the ABA may issue a standard prevention notice requiring ISPs to take all reasonable steps to prevent users from accessing the content. Alternatively, if there is a relevant industry code of practice, ISPs must comply with that code. The code currently registered requires an ISP to provide an approved filter to its clients.

84 The Act provides ISPs with an immunity with respect to State and Territory law, and any rule of common law or equity (but not Commonwealth statutes) that would subject ISPs to liability for content where they were not aware of its nature, or which would require the ISP to monitor, make inquires about or keep records of internet content hosted or carried.[100] The Act also provides internet service providers and content hosts with immunity from civil proceedings for acting in compliance with the regulatory scheme established by the Act.[101]

---

[99] Prohibited content is determined according to classification by the Classification board.

[100] Broadcasting Services Amendment (Online Services) Act 1999 (Cth) s 91.

[101] Broadcasting Services Amendment (Online Services) Act 1999 (Cth) s 88.

France

85 France has recently passed a law[102] clarifying the responsibilities of website hosts.[103] The Freedom of Communication Act proposes a general principle that hosts are not responsible for third party content. However, they must keep proper records that will allow the author of the content to be identified. Under the new law:

- Content providers are required to identify themselves to the public by putting their details on the website. If the provision of content is not a professional activity, the content provider is allowed to restrict identification to the host provider.
- Access providers and host providers are required to keep track of data allowing a content provider to be identified. This information may only be provided to a judge.
- ISPs may be made liable if they do not delete content when told to do so by a judge, or if they have failed to undertake the "appropriate diligences" when informed by a third party that they are hosting allegedly illegal content, or content that may cause a prejudice to the third party.
- Hosts are required to offer their clients at least a filter allowing them to screen out undesirable sites.

Germany

86 Germany has recently enacted legislation that clarifies the civil and criminal liability of ISPs for third party content.[104] The legislation divides the various players into five categories: Content Providers, Access Providers, Service Providers, Telecommunication Carriers and Users. A Service Provider enables the Content Provider to publish information on the internet via its server, online connections and software. An Access Provider grants Users access to the internet.

---

[102] Loi no 2000-719 relative à la liberté de communication.

[103] For third party content generally, not just offensive third party content. The law was prompted by a case in which an ISP was held liable when one of its subscribers posted nude images of a model on a website without the model's consent. The ISP was unaware of the posting. See "Les hébergeurs du Net sous surveillance" *Le Figaro*, Paris, France, 7 July 2000, 10.

[104] This legislation consists of over 20 statutes at both federal and state level. It is extensively discussed by Lothar Determann in "The New German Internet Law" (1998) 22 Hastings Intl & Comp L Rev 113.

87 A Service Provider is only liable for illegal content that it channels onto the internet if it is aware of the substance of the communication and if it is possible and acceptable[105] for the Service Provider to prevent the publication of the unlawful contents on the internet. An Access Provider is generally not liable for the content to which it provides access. However, if an Access Provider selects or promotes certain content it can qualify as an additional, secondary Content Provider with ensuing liability; for example, if it installs a hyperlink to a pornography site with a message saying "If you want to see more child pornography, visit site X". An Access Provider may be ordered by a court or a government agency to prevent the distribution of certain content to users if it is possible and commercially reasonable to do so, and if the agency is unable to directly sanction the responsible Content Provider or Service Provider.

Singapore

88 The Singapore Broadcasting Authority (SBA) has responsibility for regulating internet use in Singapore.[106] The SBA has a three-pronged approach: public education, encouraging industry self-regulation, and instituting a light-touch policy framework for regulating content. The policy framework is delivered through a Class Licensing Scheme and Internet Code of Practice. Licensing focuses on eliminating objectionable content. Under the scheme, ISPs[107] are required to register with the SBA and Internet Content Providers (ICPs)[108] must register if their webpages are set up primarily to promote political or religious causes. ISPs and ICPs must use their best efforts to comply with the Code and must act to ensure that nothing is included in any broadcasting service which offends against good taste, or works against public interest, public order or national harmony.

---

[105] The term "acceptable" is not defined but according to Determann, above n 104, 152, it appears in many German statutes and is generally interpreted to require a balancing of conflicting interests.

[106] For a discussion of internet regulation in Singapore see JC Rodriguiz "A Comparative Study of Internet Content Regulations in the United States and Singapore: The Invincibility of Cyberporn" (2000) 1 APLPJ 9; see <http://www.hawaii.edu/aplpj> (last accessed 30 November 2000).

[107] ISPs include those who function as a main gateway to the internet, such as schools, public libraries, cybercafes and service providers.

[108] ICPs are defined as information providers on the world wide web and include web authors, web publishers and web server administrators.

89 ISPs are not required to monitor the internet or its users. However, they must limit access to 100 high-impact pornographic sites identified by the SBA, and they are encouraged to take their own initiatives against offensive content through "Acceptable Use Policies" and by exercising judgment as to which newsgroups to subscribe to and make available to their users. ISPs must deny access to sites that have been identified by the SBA as possessing prohibited material. They must also furnish such information and such undertakings as the SBA may require.

90 ICPs are not required to monitor the internet or to pre-censor content. However, an ICP must bar access to prohibited materials when directed by the SBA. If an ICP is responsible for discussions on websites with public access, then the ICP is advised to choose themes according to the Code and exercise editorial judgment accordingly.

United States

91 The United States has generally supported self-regulation in relation to the internet. However, Congress has attempted to legislate in order to limit or prevent harm to minors. In 1996 the United States Congress passed the Communications Decency Act 1996 which criminalised the knowing transmission of adult-oriented material to people under 18 years of age. The Act also overturned *Stratton Oakmont v Prodigy Services*,[109] which held that an ISP was a publisher (and therefore liable in defamation) because it attempted to filter obscene and derogatory messages from the bulletin board that it operated. The Legislature was concerned that ISPs be given an incentive to attempt to control such material, rather than incentives to take a hands-off role. The Communications Decency Act 1996 states that no provider or user of an interactive computer service "shall be treated as the publisher or speaker of any information provided by any another information content provider".[110]

92 The Communications Decency Act 1996 was subsequently challenged as unconstitutional and parts were struck down by the Supreme Court.[111] Congress then passed the Child Online

---

[109] 23 Media L Rep (BNA) 1794 (NY Sup Ct May 24, 1995).

[110] Communications Decency Act 1996, s 230.

[111] *Reno v ACLU*, 117 S Ct 2329, 521 US 844, 138.

Protection Act 1998 in an attempt to enact constitutionally viable restrictions on the transmission via the internet of harmful content to minors. The Act contains status-based exemptions for telecommunications carriers, internet access providers and internet information location tool providers that refer or link users to an online location on the world wide web.[112] The Act further exempts persons "similarly engaged in the transmission, storage, retrieval, hosting, formatting, or transmission of a communication made by another . . ." provided that they do not select or alter content except by deleting it.[113] The Act requires ISPs to notify customers of the commercial availability of parental control technologies to limit the access of minors to harmful material. This Act has also been challenged as unconstitutional and a preliminary injunction was granted in February 1999.[114] The Justice Department has filed an appeal.

93 The Protection of Children from Sexual Predators Act 1998 (US) strengthens existing laws protecting children from sexual predators by adapting them to current technology. The Act imposes a duty on ISPs to report to federal law enforcement officials violations of federal child sexual exploitation laws involving child pornography where an ISP obtains knowledge of facts or circumstances that make it apparent that such violations have occurred. The Act also prohibits ISPs from knowingly transferring obscene material to individuals known to be under the age of 16. ISPs are not required to monitor their users' content and are protected from civil liability if they act in good faith to comply with the Act.

Common themes

94 A number of common themes may be noted in these various approaches to the regulation of offensive internet content.

- ISPs have knowledge-based liability for objectionable content provided by third parties.
- ISPs are not required to monitor for objectionable content.
- ISPs are encouraged to provide filters to clients and, in particular, parents.

---

[112] Child Online Protection Act 1998, s 231(b)(1)–(b)(3).

[113] Child Online Protection Act 1998, s 231(b)(4).

[114] *ACLU v Reno*, No 98-CV-5591, (ED Pa 2/1/99).

- Attempts to regulate to control objectionable content focus on creating schemes that bring objectionable content to the attention of ISPs, rather than strict liability offences.

95 The Commission recommends that these issues be kept under review by the Ministry of Justice. The Commission has sought a reference from the Minister of Justice to do further work on the legal issues raised by the distribution of child pornography, including the exchange of this material over the internet. The Commission hopes to receive a reference in due course.

8
Transport documentation

96 In ECom 2 the Commission requested submissions on whether articles 16 and 17 of the UNCITRAL Model Law on Electronic Commerce should be adopted by New Zealand.[115] These articles deal with transportation documents, and provide that certain actions in relation to the carriage of goods can be performed electronically. The Commission reached the preliminary conclusion that New Zealand did not need to adopt these articles, but that a final recommendation would be made once the outcome of work proposed at the 32nd UNCITRAL session, and further submissions, had been considered.[116]

Submissions

97 Submissions on this issue were unanimous in the conclusion that no legislation was required at this stage to facilitate electronic contracts for the carriage of goods. The Commercial and Business Law Committee of the New Zealand Law Society noted that the establishment of electronic negotiable instruments could be achieved by contractual means within the appropriate market; for example, as established by the Bolero project. The Committee distinguished between shipping documentation and statutory registry systems (such as those set out under the Motor Vehicle Securities Act 1989 and the Personal Property Securities Act 1999) which tended to record consumer or small business transactions, generally within New Zealand.[117]

International work

98 At its 32nd session (May–June 1999) UNCITRAL raised the possibility of further work on the topic of transport law.[118] Since

[115] ECom 2, chapter 4.

[116] ECom 2, paras 69 and 77.

[117] Submission of Commercial and Business Law Committee of the New Zealand Law Society, dated 19 July 2000.

[118] A/54/17, report of the 32nd session; noted ECom 2, para 69.

then, the UNCITRAL Secretariat has been working with the Comité Maritime International, gathering information on the problems in transport law that arise in practice, including the "dematerialisation of documents of title".[119] The Secretariat had noted that although bills of lading were still used, the actual carriage of goods by sea sometimes represented only a fragment of an act of international transport of goods, which was increasingly a warehouse-to-warehouse operation. It was felt that the current broadly based project should be extended to include an updated liability regime.[120] UNCITRAL requested that the Secretariat present a report at the next session (scheduled for 25 June–13 July 2001) identifying issues in transport law in respect of which UNCITRAL might undertake further work and, to the extent possible, also presenting possible solutions.[121]

Bolero project

99 The Bolero project, discussed in this Commission's earlier reports on electronic commerce,[122] started from the assumption that there was no electronic equivalent to a negotiable document of title, therefore a closed system was required that achieved the same result (certainty of title) through electronic means. The internet-based bolero.net became operative in September 1999 and provides a common, open system by which businesses can exchange trade data and documentation electronically.[123]

Conclusion

100 Given that the transport law work identified by UNCITRAL is unlikely to be concluded in the near future, and the success of market-driven trade infrastructures such as Bolero, the Commission reiterates its conclusion that articles 16 and 17 of the UNCITRAL Model Law need not be enacted into New Zealand law at this time. The Commission is supported by submissions in this conclusion.

---

[119] A/55/17, report of 33rd session, para 386 and chapter 10.

[120] Above n 119, paras 422–424.

[121] Above n 119, para 427.

[122] See ECom 1, paras 124–125 and ECom 2, para 71.

[123] See further <www.bolero.net> (last accessed 29 November 2000).

9
Electronic signatures

101 In ECom 2[124] we summarised developments overseas since publication of ECom 1 and proceeded to recommend that:

- Immediate barriers to electronic commerce caused by statutory references to "signing" be removed by a provision akin to article 7 of the Model Law on Electronic Commerce.[125]
- No further action be taken to deal with what we termed "enhanced electronic signatures" – we proposed that that issue await development of the work of the UNCITRAL Working Group on Electronic Commerce.[126]
- No legislation should be introduced to provide a framework for Public Key Infrastructure (PKI) for digital signatures, notwithstanding that some countries had adopted prescriptive legislation for that purpose.[127]

102 The Electronic Transactions Bill, as introduced into Parliament, has done two things with regard to electronic signatures. First it has adopted, as the starting point, the reliability criterion from article 7 of the Model Law on Electronic Commerce. But then it has built upon article 7 by adopting what are currently articles 6(3) and (4) of the draft UNCITRAL Model Law on Electronic Signatures.[128] This has been done to bring about a greater degree of predictability for users and courts in determining whether an electronic signature will meet the statutory requirement for a signature in any given circumstance. To some extent, what has been done in draft article 6(3) is to provide greater predictability with respect to both signatures required by law generally and also those signatures which, as a matter of law, require some added form of security to vouchsafe the integrity of the document which is

[124] ECom 2, chapter 9, paras 147–152 and appendix E.

[125] ECom 2, para 153.

[126] ECom 2, para 154.

[127] ECom 2, para 155.

[128] See clause 24 of the Electronic Transactions Bill reproduced in appendix A.

being signed. While the provisions of draft articles 6(3) and (4) were drafted having regard to what actually occurs in a PKI environment, they are drafted in technologically neutral terms.

Draft UNCITRAL Model Law on Electronic Signatures – reliability of signatures

103 ECom 2 was published in November 1999. Since then, the UNCITRAL Working Group on Electronic Commerce has held two sessions to complete its work on electronic signatures: the first meeting took place in New York, 14–25 February 2000; the second took place in Vienna, 18–29 September 2000. At both of those meetings New Zealand was represented by Paul Heath QC.

104 A breakthrough occurred at the UNCITRAL Working Group held in New York in February 2000. This breakthrough occurred because participants were able to agree upon a formula to create a rebuttable presumption that a particular type of electronic signature would be considered reliable for the purpose of meeting a legal requirement for a signature if the following three criteria were met:

- the means of creating the electronic signature were linked to the signatory and to no other person;
- the means of creating the electronic signature were, at the time of signing, under the control of the signatory and of no other person; and
- any alteration to the electronic signature made after the time of signing was detectable.

105 Although there was general agreement on the formula set out above, there were still two major issues that required resolution:

- The need to craft the article in a manner which would meet the concerns of some legal systems about the use of presumptions and leave open the ability of parties to establish reliability or non-reliability of an electronic signature through other means.
- The need of some legal systems to ensure that where a legal requirement for a signature existed, any alteration made to the information to which the electronic signature related (as well as the electronic signature) were detectable.

106 These two points were answered in the following ways:

- In relation to the first issue, by adding a new sub-rule which made it clear that nothing limited the ability of any person to establish in any other way the reliability of an electronic signature or, indeed, to adduce evidence of the non-reliability of an electronic signature.

- In relation to the second issue, by inserting another new sub-rule which made it clear that where the purpose of a legal requirement or signature was to provide an assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing must also be detectable. In some jurisdictions a legal requirement for a signature will always carry a requirement to provide assurance as to the integrity of the information to which the signature relates.

107 After consultation with experts in New Zealand, it became clear that this formulation was acceptable from a technical point of view, and that it would be possible for affidavits to be drafted in advance for use in instances (for example, in summary judgment applications) where it may be necessary to identify the processes which had been undertaken with a view to proving that the presumption was satisfied. In any given case the affidavit evidence would still need to go on to demonstrate that the processes put in place for ensuring that the signature was affixed electronically had, in fact, been followed. However, what this formula created was an ability to predict, before any transaction was entered into, whether the electronic signature was likely to reach the standard of reliability required.

108 This formulation was approved, in general terms, at the meeting of the UNCITRAL Working Group on Electronic Commerce held in Vienna in September 2000. It is now captured in articles 6(3) and (4) of the draft Model Law on Electronic Signatures.[129] Some minor modifications were made to replace the term "the means of creating an electronic signature" with the phrase "the signature creation data" to ensure consistency of approach between articles in the draft Model Law on Electronic Signature referring to (on the one hand) the reliability of electronic signatures and (on the other) the conduct expected from Certification Service Providers who provide services to support the verification of an electronic signature.[130] The same need for consistency does not arise under the Electronic Transactions Bill and we support reference to the term "means of creating an electronic signature" in clause 24(1) of the Bill.

---

[129] See appendix B. Note that the Working Group decided to call the draft a Model Law rather than use the term "Uniform Rules" which was the working title of the work on electronic signatures.

[130] Compare articles 6 and 9 of the draft Model Law on Electronic Signatures.

109 The Commission is pleased to support the proposed provisions of the Electronic Transactions Bill which provide greater predictability for determining the reliability of an electronic signature for meeting legal requirements for a signature. In particular, the Commission is pleased to lend its support to provisions which are based upon the draft Model Law on Electronic Signatures.

Draft UNCITRAL Model Law on Electronic Signature – other aspects

110 The scheme of the draft UNCITRAL Model Law on Electronic Signatures[131] is as follows:

- The draft Model Law repeats, in articles 1, 3, 4 and 5, a number of principles which underpin the UNCITRAL Model Law on Electronic Commerce: scope of application (article 1), technological neutrality (article 3), interpretation in accordance with international origins (article 4) and party autonomy (article 5).
- Article 2 provides definitions of the terms "electronic signature", "certificate", "data message", "certification service provider" and "relying party".
- The reliability of electronic signatures used to meet legal requirements for a signature is dealt with in article 6. Article 7 provides that an electronic signature will be regarded as meeting the legal requirement for a signature if a particular type of electronic signature is used which meets a determination made by an organisation specified by the enacting State and which is consistent with recognised international standards.
- Articles 8, 9, 10 and 11 of the draft Model Law make reference to the use of verifying authority for electronic signatures. These articles proceed upon the assumption that an independent trusted third party is being used to verify the use of an electronic signature by a signatory and that reliance is being placed on that verification by a third party. Article 8 deals with obligations cast upon a signatory; article 9 deals with obligations cast upon a certification service provider (sometimes called a certification authority) and article 11 deals with the conduct of the relying party. Article 10 provides some amplification on the concept of "trustworthy systems, procedures and human resources" required to be used by certification service providers by article 9(1)(f).

---

[131] Set out in full in appendix B.

- Article 12 provides a basis for the recognition of foreign certificates and electronic signatures.

111 It is proposed to discuss briefly the tripartite arrangements involving signatories, certification service providers and relying parties, although no recommendation is made by the Commission for enactment of legislation of this type in New Zealand. The Commission does, however, commend to those involved in electronic commerce the provisions of articles 8–11 of the draft Model Law as setting out standards of best practice which are likely to be relevant to the assessment, by a court or arbitral tribunal, of contractual or tortious duties owed by parties in those roles. We also discuss briefly the cross-border recognition provisions which we recommend be considered for enactment in New Zealand at some time in the future.

Certification process

112 The provisions of articles 8, 9 and 11 are intended to apply where a signature is intended to have legal effect (for example, on a contract rather than a mere autograph) whether or not there is a legal requirement for a signature. Thus, the rules contained in articles 8, 9 and 11 have wider application than the rules contained in article 6, which are limited to legal requirements for a signature.

113 Where a signatory has a code or private key available to create an electronic signature, that person must exercise reasonable care to avoid unauthorised use of the code or key and, without undue delay, notify any person that may reasonably be expected to rely on or to provide services in support of the electronic signature if the code or key has been compromised or if circumstances known to the signatory are such as to give rise to a substantial risk that the signature creation data may have been compromised.[132] Further, where a certificate is used to support the electronic signature, the signatory must use reasonable care to ensure the accuracy and completeness of all material representations which are relevant to the certificate throughout its life cycle or which are to be included in the certificate.[133] A signatory is liable for its failure to satisfy those requirements.[134] Liability is a matter to be determined by reference to applicable law.

---

[132] UNCITRAL draft Model Law on Electronic Signatures, articles 8(1)(a) and (b).

[133] Above n 132, article 8(1(c).

[134] Above n 132, article 8(2).

114 A simple example suffices to explain the nature of the obligations on signatories. Let us suppose that X uses a card to obtain cash from an automatic teller machine. X has a PIN to gain access to his or her bank account. If X gives someone else the PIN (that is, the relevant code) and that person is able to access the account, the signatory is likely to be liable whereas if he or she has used reasonable care to safeguard the PIN, the user is unlikely to be liable. In this respect, the code or key used to create the electronic signature is akin to a PIN.

115 A person who carries on business as a certification services provider must act in accordance with representations made by that business with respect to its policies and practices, and exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle or which are included in the certificate.[135] From the certificate provided a relying party must be able to ascertain:

- the identity of the certification service provider;
- that the signatory identified in the certificate had control of the signature creation data at the time when the certificate was issued; and
- that the signature creation data was valid at or before the time when the certificate was issued.[136]

116 In addition, from reasonably accessible means (including incorporation by reference) the certification services provider must disclose to a relying party:

- the method used to identify the signatory;
- any limitation on the purpose or value for which the signature creation data or the certificate may be used;
- that the signature creation data are valid and have not been compromised;
- any limitation on the scope or extent of liability stipulated by the certification service provider;
- whether means exist for the signatory to give notice of compromise under draft article 8(1)(b); and
- whether a timely revocation service is offered.[137]

---

[135] Above n 132, articles 9(1)(a) and (b).

[136] Above n 132, article 9(1)(c).

[137] Above n 132, article 9(1)(d).

117 Where means exist for the signatory to give notice of compromise or where timely revocation services are offered, the certification service provider must ensure the availability of those services but not necessarily provide those services itself.[138] Finally, trustworthy systems, procedures and human resources must be used to perform its services.[139]

118 A certification service provider will be liable for its failure to satisfy those obligations with the extent of liability to be fixed in accordance with applicable law.[140]

119 So far as a relying party is concerned, it will bear the legal consequences of its failure:

- to take reasonable steps to verify the reliability of an electronic signature; or
- to take reasonable steps to verify the validity, suspension or revocation of the certificate and observe any limitation with respect to the certificate, where the electronic signatory is supported by a certificate.[141]

Cross-border recognition

120 A new provision was inserted into the draft Model Law on Electronic Signatures at the September 2000 meeting of the UNCITRAL Working Group on Electronic Signatures held in Vienna. This related to the recognition of foreign certificates and electronic signatures. In determining whether, or to what extent, a certificate or an electronic signature is legally effective, it will be impermissible to have regard purely to the geographic location where the certificate was issued or the electronic signature created or used or to the place of business of the issuer or signatory.[142] This prohibition is intended to relate solely to discrimination on the grounds of creation or issue or location out of the particular jurisdiction; it is not intended to deny consideration of whether or not the particular electronic signature or certificate was validly issued or used within that jurisdiction.

---

[138] Above n 132, article 9(1)(e).

[139] Above n 132, articles 9(1)(f) and 10.

[140] Above n 132, article 9(2).

[141] Above n 132, article 11.

[142] Above n 132, article 12(1).

121 The test for adequacy of a certificate or electronic signature issued or created in another country is whether that country's law for domestic certificates and signatures offers a substantially equivalent level of reliability to that required under New Zealand law.[143] As matters presently stand, the level of reliability required under New Zealand law would be judged by the courts by reference to common law criteria, which do not discriminate by reference to location.

122 In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability the courts may have regard to recognised international standards and any other relevant factors.[144] Where parties agree to use certain types of electronic signatures or certificates, that agreement shall be recognised unless the agreement would not be valid or effective under applicable law.[145]

123 Although the Commission believes that the sentiments expressed in draft article 12 will be given effect by the courts in New Zealand, there may be some merit in adopting draft article 12 as part of New Zealand law if that article is ultimately approved by UNCITRAL and enacted by a number of our major trading partners. We recommend that the Ministry of Economic Development monitor this issue to determine whether a cross-border recognition provision is required in the future.

Attribution

124 In paragraph 336 of ECom 2 we indicated that we proposed to revisit the desirability of enacting a provision akin to article 13 of the Model Law On Electronic Commerce in this report.[146] We deferred this issue so that we could assess whether anything arising out of the UNCITRAL work on electronic signatures would affect our final recommendation.[147]

---

[143] Above n 132, article 12(2).

[144] Above n 132, article 12(4).

[145] Above n 132, article 12(5).

[146] See ECom 1, paras 62, 94–99 and ECom 2, paras 48–52; see also *Guide to Enactment of Model Law On Electronic Commerce*, paras 83–92, reproduced ECom 2, 192–195.

[147] ECom 2, para 52, 2nd point.

125 Nothing arose in the course of the UNCITRAL work on electronic signatures which takes the matter any further. We adhere to the approach set out in ECom 2 and prefer questions of attribution to be dealt with by domestic law, whether written or unwritten, rather than by a specific provision in the Electronic Transactions Bill for the reasons given in ECom 2.[148]

---

[148] ECom 2, paras 48–52.

APPENDIX A

Electronic Transactions Bill

Contents

The Parliament of New Zealand enacts as follows

1 Title

This Act is the Electronic Transactions Act **2000**.

2 Commencement

(1) This Act (except **sections 14 (3) and 35**) comes into force on a date to be appointed by the Governor-General by Order in Council.

(2) **Sections 14 (3) and 35** come into force on the day after the date on which the Act receives the Royal assent.

Part 1
Preliminary

3 Purpose

The purpose of this Act is to facilitate the use of electronic technology by–

(a) reducing uncertainty regarding–

(i) the legal effect of information that is in electronic form or that is communicated by electronic means; and

(ii) the time and place of dispatch and receipt of electronic communications; and

(b) providing that certain paper-based legal requirements may be met by using electronic technology that is functionally equivalent to those legal requirements.

4 Overview

In this Act,–

(a) matters concerning the legal effect of information that is in electronic form or that is communicated by electronic means are set out in **section 8**:

(b) default rules about the time and place of dispatch and receipt of electronic communications are set out in **sections 9 to 13**:

(c) key provisions concerning the use of electronic technology to meet certain legal requirements are set out in **sections 14 to 17**:

(d) provisions that specify certain legal requirements that may be met by using electronic technology, and how they may be met, are set out in **sections 18 to 32**.

5 Interpretation

In this Act, unless the context otherwise requires,–

data storage device means any article or device (for example, a disk) from which information is capable of being reproduced, with or without the aid of any other article or device

electronic includes electrical, digital, magnetic, optical, electromagnetic, biometric and photonic

electronic communication means a communication by electronic means

information includes information (whether in its original form or otherwise) that is in the form of a document, a signature, a seal, data, text, images, sound, or speech

information system has the meaning set out in **section 10(2)**

legal requirement has the meaning set out in **section 15(2)**

transaction includes–

(a) a transaction of a non-commercial nature:

(b) a single communication:

(c) the outcome of multiple related communications.

6 Further provision relating to interpretation

In interpreting this Act, reference may be made to–

(a) the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law on 16 December 1996:

(b) any document that relates to the Model Law that originates from the United Nations Commission on International Trade Law, or its working group for the preparation of the Model Law.

7 Act binds the Crown

This Act binds the Crown.

Part 2
Improving certainty in relation to electronic information and electronic communications

Validity

8 Validity of information

To avoid doubt, information is not denied legal effect solely because it is–

(a) In electronic form or is communicated by electronic means:

(b) Referred to in an electronic communication that is intended to give rise to that legal effect.

Default rules about dispatch and receipt of electronic communications

9 When default rules in sections 10 to 13 apply

Sections 10 to 13 apply to an electronic communication except to the extent that–

(a) the parties to the communication otherwise agree:

(b) an enactment provides otherwise.

10 Time of dispatch

(1) An electronic communication is taken to be dispatched at the time the electronic communication first enters an information system outside the control of the originator.

(2) For the purposes of **sections 10 and 11, information system** means a system for producing, sending, receiving, storing, displaying, or otherwise processing electronic communications.

11 Time of receipt

An electronic communications is taken to be received,–

(a) in the case of an addressee who has designated an information system for the purpose of receiving electronic communications, at the time the electronic communication enters that information system; or

(b) in any other case, at the time the electronic communication comes to the attention of the addressee.

12 Place of dispatch

An electronic communication is taken to be dispatched from–

(a) the originator's place of business; or

(b) if the originator has more than 1 place of business,–

(i) the place of business that has the closest relationship with the underlying transaction; or

(ii) if there is no place of business to which **subparagraph (i)** applies, the originator's principal place of business; or

(c) in the case of an originator who does not have a place of business, the originator's ordinary place of residence.

13 Place of receipt

An electronic communication is taken to be received at–

(a) the addressee's place of business; or

(b) if the addressee has more than 1 place of business,–

(i) the place of business that has the closest relationship with the underlying transaction; or

(ii) if there is no place of business to which **subparagraph (i)** applies, the addressee's principal place of business; or

(c) in the case of an addressee who does not have a place of business, the addressee's ordinary place of residence.

Part 3
Application of legal requirements to electronic transactions

Subpart 1 – Preliminary

14 When Part applies

(1) Subject to **subsection (2)**, this Part applies to every enactment that is part of the law of New Zealand and that is passed either before or after the commencement of this Act.

(2) This Part does not apply to–
  (a) an enactment that requires information to be recorded, given, produced, or retained, or a signature to be given, or a signature or seal to be witnessed–
    (i) in accordance with particular electronic technology requirements; or
    (ii) on a particular kind of data storage device; or
    (iii) by means of a particular kind of electronic communications:
  (b) the enactments specified in **Part 1 of the Schedule**:
  (c) the provisions of enactments specified in **column 2 of Part 2 of the Schedule**:
  (d) the provisions of enactments that are described in **Part 3 of the Schedule**:
  (e) the provisions of the enactments that are described in **Part 4 of the Schedule** except to the extent that rules of a court, or guidelines issued with the authority of a court or tribunal, specified in that Part of the Schedule provide for the use of electronic technology in accordance with this Part.

(3) The Governor-General may, by Order in Council, amend the Schedule or repeal the Schedule and substitute a new schedule.

15 Satisfaction of legal requirements through use of electronic technology

(1) A legal requirement can be met using electronic technology if–
  (a) the provisions in **subpart 2** are satisfied; and
  (b) any conditions prescribed by any regulations made under **section 35** are satisfied.

(2) For the purpose of this Part, **legal requirement**–
  (a) means a provision–
    (i) in an enactment to which this Part applies; and
    (ii) of a kind that is referred to in **subpart 2**; and
  (b) includes a provision that imposes an obligation or that provides consequences depending on whether or not the provision is complied with.

16 Consent to use of electronic technology

(1) Nothing in this Part requires a person to use, provide, or accept information in an electronic form without that person's consent.

(2) For the purposes of this Part,–
  (a) a person may consent to use, provide, or accept information in an electronic form subject to conditions regarding the form of the information or the means by which the information is produced, sent, received, processed, stored, or displayed:
  (b) consent may be inferred from a person's conduct.

(3) **Subsections (1) and (2)(a)** are for the avoidance of doubt.

17 When integrity of information maintained

For the purposes of this Part, the integrity of information is maintained only if the information has remained complete and unaltered, other than the addition of any endorsement, or any immaterial change, that arises in the normal course of communication, storage, or display.

Subpart 2 – Legal Requirements

Writing

18 Requirement that information be in writing

A legal requirement that information be in writing is met by information that is in electronic form if the information is readily accessible so as to be usable for subsequent reference.

19 Requirement to record information in writing

A legal requirement that information be recorded in writing is met by recording the information in electronic form if the information is readily accessible so as to be usable for subsequent reference.

20 Requirement to give information in writing

(1) A legal requirement to give information in writing is met by giving the information in electronic form, whether by means of an electronic communication or otherwise, if–

(a) the information is readily accessible so as to be usable for subsequent reference; and

(b) the person to whom the information is required to be given consents to the information being given in electronic form and by means of an electronic communication, if applicable.

(2) If **subsection (1)** applies, a legal requirement to provide multiple copies of the information to the same person at the same time is met by providing a single electronic version of the information.

(3) **Subsection (1)** applies to a legal requirement to give information even if that information is required to be given in a specified manner, for example by filing, sending, serving, delivering, lodging, or posting that information.

(4) A legal requirement to give information includes, for example,–

(a) making an application:

(b) making or lodging a claim:

(c) giving, sending, or serving a notification:

(d) lodging a return:

(e) making a request:

(f) making a declaration:
(g) lodging or issuing a certificate:
(h) making, varying, or cancelling an election:
(i) lodging an objection:
(j) giving a statement of reasons.

21 Additional requirements relating to information in writing
To avoid doubt, a legal requirement relating to the form or layout of, or the materials to be used for writing, information, or any similar requirement, need not be complied with in order to meet a legal requirement to which any of **sections 18 to 20** apply.

Signatures

22 Requirement for signature
(1) Subject to **subsection (2)**, a legal requirement for a signature other than a witness' signature is met by means of an electronic signature if the electronic signature–
  (a) adequately identifies the signatory and adequately indicates the signatory's approval of the information to which the signature relates; and
  (b) is as reliable as is appropriate given the purpose for which, and the circumstances in which, the signature is required.
(2) A legal requirement for a signature is not met by means of an electronic signature unless, in the case of a signature on information that is required to be given to a person, that person consents to receiving the electronic signature.

23 Requirement that signature or seal be witnessed
(1) Subject to **subsection (2)**, a legal requirement for a signature or a seal to be witnessed is met by means of a witness' electronic signature, if–
  (a) in the case of the witnessing of a signature, the signature is an electronic signature that complies with **section 22**; and
  (b) in the case of the witnessing of a signature or a seal, the electronic signature of the witness–
    (i) adequately identifies the witness and adequately indicates that the signature or seal has been witnessed; and
    (ii) is as reliable as is appropriate given the purpose for which, and the circumstances in which, the witness' signature is required.
(2) A legal requirement for a signature or seal to be witnessed is not met by means of a witness' electronic signature unless, in the case of a witness' signature on information that is required to be given to a person, that person consents to receiving the witness' electronic signature.

24 Presumption about reliability of electronic signatures

(1) For the purposes of **sections 22 and 23**, it is presumed that an electronic signature is as reliable as is appropriate if–

(a) the means of creating the electronic signature is linked to the signatory and to no other person; and

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

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

(d) where the purpose of the legal 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.

(2) **Subsection (1)** does not prevent any person from proving on other grounds or by other means that an electronic signature–

(a) is as reliable as is appropriate; or

(b) is not as reliable as is appropriate.

Retention

25 Requirement to retain document or information in paper form

(1) A legal requirement to retain information that is in paper or other non-electronic form is met by retaining an electronic form of the information if–

(a) the electronic form provides a reliable means of assuring the maintenance of the integrity of the information; and

(b) the information is readily accessible so as to be usable for subsequent reference.

(2) **Subsection (1)** applies to information that is a public record within the meaning of the Archives Act 1957 only if the Chief Archivist has approved the retention of that information in electronic form.

(3) To avoid doubt, if information is retained in electronic form in accordance with **subsection (1)**, the paper or other non-electronic form of that information need not be retained.

26 Requirement to retain information in electronic form

Subject to **section 27**, a legal requirement to retain information that is in electronic form is met by retaining the information–

(a) in paper or other non-electronic form if the form provides a reliable means of assuring the maintenance of the integrity of the information; or

(b) in electronic form if–

(i) the electronic form provides a reliable means of assuring the maintenance of the integrity of the information; and

(ii) the information is readily accessible so as to be usable for subsequent reference.

27 Extra conditions for electronic communications

In addition to the conditions specified in **section 26**, if a person is required to retain information that is contained in an electronic communication,–

(a) the person must also retain such information obtained by that person as enables the identification of–

(i) the origin of the electronic communication; and

(ii) the destination of the electronic communication; and

(iii) the time when the electronic communication was sent and the time when it was received; and

(b) the information referred to in **paragraph (a)** must be readily accessible so as to be usable for subsequent reference.

Provision and production of, and access to, information

28 Requirement to provide or produce information in paper form

A legal requirement to provide or produce information that is in paper or other non-electronic form is met by providing or producing the information in electronic form, whether by means of an electronic communication or otherwise, if–

(a) the form and means of the provision or production of the information reliably assures the maintenance of the integrity of the information, given the purpose for which, and the circumstances in which, the information is required to be provided or produced; and

(b) the information is readily accessible so as to be usable for subsequent reference; and

(c) the person to whom the information is required to be provided or produced consents to the information being provided or produced in an electronic form and, if applicable, by means of an electronic communication.

29 Requirement to provide or produce information in electronic form

A legal requirement to provide or produce information that is in electronic form is met by providing or producing the information–

(a) in paper or other non-electronic form; but, if the maintenance of the integrity of the information cannot be assured, the person who must provide or produce the information must–

(i) notify every person to whom the information is required to be provided or produced of that fact; and

(ii) if requested to do so, provide or produce the information in electronic form in accordance with **paragraph (b)**; or

(b) in electronic form, whether by means of an electronic communication or otherwise, if–

(i) the form and means of the provision or production of the information reliably assures the maintenance of the integrity of the information, given the purpose for which, and the circumstances in which, the information is required to be provided or produced; and

(ii) the information is readily accessible so as to be usable for subsequent reference; and

(iii) the person to whom the information is required to be provided or produced consents to the provision or production of the information in an electronic form and,if applicable, by means of an electronic communication.

30 Requirement to provide access to information in paper form

A legal requirement to provide access to information that is in paper or other non-electronic form is met by providing access to the information in electronic form if–

(a) the form and means of access to the information reliably assures the maintenance of the integrity of the information, given the purpose for which, and the circumstances in which, access to the information is required to be provided; and

(b) the person to whom access is required to be provided consents to accessing the information in that electronic form.

31 Requirement to provide access to information in electronic form

A legal requirement to provide access to information that is in electronic form is met by providing access to the information–

(a) in paper or other non-electronic form; but, if the maintenance of the integrity of the information cannot be assured, the person who must provide access to the information must–

(i) notify every person to whom access is required to be provided of that fact; and

(ii) if requested to do so, provide access to the information in electronic form in accordance with **paragraph (b)**; or

(b) in electronic form, whether by means of an electronic communication or otherwise, if–

(i) the form and means of access to the information reliably assures the maintenance of the integrity of the

information, given the purpose for which, and the circumstances in which, access to the information is required to be provided; and

(ii) the person to whom access is required to be provided consents to accessing the information in that electronic form.

Originals

32 Originals

A legal requirement to compare a document with an original document may be met by comparing that document with an electronic form of the original document if the electronic form reliably assures the maintenance of the integrity of the document.

Subpart 3 – Miscellaneous

33 Content requirements

Nothing in this Part affects any legal requirement to the extent that the requirement relates to the content of information.

34 Copyright

The copyright in a work is not infringed by any of the following acts if they are carried out for the purposes of meeting a legal requirement by electronic means:

(a) the generation of an electronic form of a document;

(b) the production of information by means of an electronic communication.

35 Regulations

The Governor-General may, by Order in Council, make regulations prescribing conditions that must be complied with in order to meet a legal requirement specified in those regulations by electronic means.

36 Related amendment to Interpretation Act 1999

Section 29 of the Interpretation Act 1999 is amended by repealing the definition of **writing**, and substituting the following definition:

"**writing** means representing or reproducing words, figures, or symbols in a visible and tangible form and medium (for example, in print)".

Schedule

s 14(2)(b), (c), (d), and (e)

Enactments and provisions excluded from Part 3

Part 1
Enactments

Citizens Initiated Referenda Act 1993 (1993 No 101)

Citizens Initiated Referenda Regulations 1995 (SR 1995/227)

Electoral Act 1993 (1993 No 87)

Electoral Regulations 1996 (SR 1996/93)

Fish and Game Council Elections Regulations 1990 (SR 1990/361)

Local Elections and Polls Act 1976 (1976 No 144)

Part 2
Provisions

Enactment	Provisions
Alcoholism and Drug Addiction Act 1966 (1966 No 97)	Section 18
Burial and Cremation Act 1964 (1964 No 75)	Section 46A
Citizenship Act 1977 (1977 No 61)	Sections 12 and 19(1)
Citizenship Regulations 1978 (SR 1978/181)	Regulation 13
Civil Aviation Act 1990 (1990 No 98)	Section 11(2) and 6(b)
Conservation Act 1987 (1987 No 65)	Section 26ZZM(2)(b)(ii)
Credit Contacts Act 1981 (1981 No 27)	Sections 16, 17, 20 (to the extent that it relates to the disclosure requirements under sections 16 and 17), 21(2) and 22(2)(a)
Credit (Repossession) Act 1997 (1997 No 85)	Sections 8, 9, 17, 18, 20, 21, 29(2)(a), 33 and 38
Criminal Justice Regulations 1985 (SR 1985/232)	Regulation 7
Dental Act 1988 (1988 No 150)	Sections 37(6) and 38(4)

Dietitians Act 1950 (1950 No 44)	Section 23(6)
Disabled Persons Community Welfare Act 1975 (1975 No 122)	Section 25F(4)
Door to Door Sales Act 1967 (1967 No 126)	Section 6(1)
Fisheries Act 1996 (1996 No 88)	Part VIII
Health Act 1956 (1956 No 65)	Sections 53A and 46
Hire Purchase Act 1971 (1971 No 147)	Sections 7, 10(1)(b) and 46
Human Tissue Act 1964 (1964 No 19)	Section 3
Medical Practitioners Act 1995 (1995 No 95)	Section 80
Mental Health (Compulsory Assessment and Treatment) Act 1992 (1992 No 46)	Sections 31, 59 to 61 and 64
Misuse of Drugs Amendment Act 1978 (1978 No 65)	Section 13C
National Parks Act 1980 (1980 No 66)	Sections 56G(2)(b) and 62(3)(a)
Occupational Therapy Act 1949 (1949 No 9)	Section 23(6)
Passports Act 1992 (1992 No 92	Section 19
Penal Institutions Regulations 2000 (SR 2000/81)	Regulation 161
Physiotherapy Act 1949 (1949 No 8)	Section 22(6)
Tuberculosis Act 1948 (1948 No 36)	Sections 9, 10 and 16
Wheat Industry Research Levies Act 1989	Schedule and Appendix of Schedule
Wildlife Act 1953 (1953 No 31)	Section 41(2)(g)

Part 3
Descriptions of Provisions of Enactments

Provisions of enactments that relate to the following:

(a) notices that are required to be given to the public:

(b) information that is required to be given in writing either in person or by registered post:

(c) notices that are required to be attached to any thing or left or displayed in any place:
(d) affidavits, statutory declarations, or other documents given on oath or affirmation:
(e) powers of attorney or enduring powers of attorney:
(f) wills, codicils, or other testamentary instruments:
(g) negotiable instruments:
(h) bills of lading:
(i) instruments or any other documents presented to, deposited with, entered on the register or filed by, the Registrar-General of Land or the Registrar of Deeds:
(j) notices or certificates required to be given to a patient or proposed patient under the Mental Health (Compulsory Assessment and Treatment) Act 1992 regarding assessments, treatments, alterations to treatments, or any review process:
(k) requirements to produce or serve a warrant or other document that authorises–
    (i) entry on premises; or
    (ii) the search of any person, place, or thing; or
    (iii) the seizure of any thing:
(l) information required in respect of any goods or services by a consumer information standard or a product safety standard or a services safety standard prescribed under the Fair Trading Act 1986:
(m) instruments or any other documents lodged with the Registrar of Ships in respect of the New Zealand Register of Ships established under the Ship Registration Act 1992.

Part 4
Provisions of Enactments Relating to Certain Courts and Tribunals

Provisions of enactments relating to the practice or procedure of any of the following:

(1) the Court of Appeal or the High Court continued by the Judicature Act 1908:

(2) District Courts continued by the District Courts Act 1947:

(3) Family Courts established under the Family Courts Act 1980:

(4) Youth Courts established under the Children, Young Persons, and Their Families Act 1989:

(5) Disputes Tribunals established under the Disputes Tribunals Act 1988:

(6) the Maori Appellate Court and the Maori Land Court continued under Te Ture Whenua Maori Act 1993:

(7) the Courts-Martial Appeal Court constituted under the Courts Martial Appeals Act 1953:

(8) Courts-Martial convened under the Armed Forces Discipline Act 1971:

(9) the Customs Appeal Authority established under the Customs and Excise Act 1996:

(10) the Catch History Review Committee established under the Fisheries Act 1996:

(11) the Quota Appeal Authority established under the Fisheries Act 1983:

(12) Land Valuation Tribunals established under the Land Valuation Proceedings Act 1948:

(13) Motor Vehicles Disputes Tribunals established under the Motor Vehicles Dealers Act 1975:

(14) the Refugee Status Appeals Authority and the Removal Review Authority continued by, and the Residence Appeal Authority established under, the Immigration Act 1987:

(15) the Social Security Appeal Authority and the Benefits Review Committees established under the Social Security Act 1964, and any Appeal Board appointed under section 53A of that Act:

(16) the Student Allowance Appeal Authority established under the Education Act 1989:

(17) the Survey Board of New Zealand constituted under the Survey Act 1986:

(18) the Tenancy Tribunal constituted under the Residential Tenancies Act 1986:

(19) the State Housing Appeal Authority constituted under the Housing Restructuring (Appeals) Regulations 2000:

(20) the Environment Court continued by the Resource Management Act 1991:

(21) the Waitangi Tribunal established under the Treaty of Waitangi Act 1975:

(22) the Dental Technicians Board and the Dental Council of New Zealand continued by, the Dentists Disciplinary Tribunal, the Clinical Dental Technicians Disciplinary Tribunal, and the Dental Technicians Disciplinary Tribunal constituted under, and Complaints Assessments Committees appointed under, the Dental Act 1988:

(23) the Dietitians Board continued by, and the Penal Cases Committee appointed under, the Dietitians Act 1950:

(24) the Medical Laboratory Technologists Board, the Medical Radiation Technologists Board, and the Podiatrists Board, continued by the Medical Auxiliaries Act 1966:

(25) the Medical Council of New Zealand continued by, the Medical Practitioners Disciplinary Tribunal constituted under, and Complaints Assessment Committees appointed under, the Medical Practitioners Act 1995:

(26) the Nursing Council of New Zealand continued by, and the Preliminary Proceedings Committee appointed under, the Nurses Act 1977:

(27) the Opticians Board continued by, and the Penal Cases Committee appointed under, the Optometrists and Dispensing Opticians Act 1976:

(28) the Pharmaceutical Society of New Zealand continued by, and the Disciplinary Committee of the Pharmaceutical Society of New Zealand appointed under, the Pharmacy Act 1970:

(29) the Physiotherapy Board continued by, and the Director of Proceedings, as defined in, the Physiotherapy Act 1949:

(30) the Plumbers, Gasfitters, and Drainlayers Board constituted under the Plumbers, Gasfitters, and Drainlayers Act 1976:

(31) the Psychologists Board continued by, and Complaints Assessment Committees established under, the Psychologists Act 1981.

APPENDIX B

Draft UNCITRAL Model Law on Electronic Signatures

(as approved by the UNCITRAL Working Group on Electronic Commerce at its thirty-seventh session, held at Vienna from 18 to 29 September 2000)

Article 1. Sphere of application

This Law applies where electronic signatures are used in the context* of commercial** activities. It does not override any rule of law intended for the protection of consumers.

*The Commission suggests the following text for States that might wish to extend the applicability of this Law:

> "This Law applies where electronic signatures are used, except in the following situations: [. . .]."

**The term "commercial" should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include, but are not limited to, the following transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road.

Article 2. Definitions

For the purposes of this Law:

(a) "Electronic signature" means data in electronic form in, affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message;

(b) "Certificate" means a data message or other record confirming the link between a signatory and signature creation data;
(c) "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;
(d) "Signatory" means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents;
(e) "Certification service provider" means a person that issues certificates and may provide other services related to electronic signatures;
(f) "Relying party" means a person that may act on the basis of a certificate or an electronic signature.

Article 3. Equal treatment of signature technologies

Nothing in this Law, except article 5, shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements referred to in article 6 (1) or otherwise meets the requirements of applicable law.

Article 4. Interpretation

(1) In the interpretation of this Law, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith.
(2) Questions concerning matters governed by this Law which are not expressly settled in it are to be settled in conformity with the general principles on which this Law is based.

Article 5. Variation by agreement

The provisions of this Law may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under applicable law.

Article 6. Compliance with a requirement for a signature

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used which is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph (1) if:
   (a) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person;
   (b) the signature creation data were, 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 legal 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) Paragraph (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 paragraph (1), the reliability of an electronic signature; or
   (b) to adduce evidence of the non-reliability of an electronic signature.

(5) The provisions of this article do not apply to the following: [. . .]

Article 7. Satisfaction of article 6

(1) [*Any person, organ or authority, whether public or private, specified by the enacting State as competent*] may determine which electronic signatures satisfy the provisions of article 6.

(2) Any determination made under paragraph (1) shall be consistent with recognized international standards.

(3) Nothing in this article affects the operation of the rules of private international law.

Article 8. Conduct of the signatory

(1) Where signature creation data can be used to create a signature that has legal effect, each signatory shall:
   (a) exercise reasonable care to avoid unauthorized use of its signature creation data;
   (b) without undue delay, notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if:
      (i) the signatory knows that the signature creation data have been compromised; or

(ii) the circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised;

(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 signatory which are relevant to the certificate throughout its life-cycle, or which are to be included in the certificate.

(2) A signatory shall be liable for its failure to satisfy the requirements of paragraph (1).

Article 9. Conduct of the certification service provider

(1) Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall:

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

(b) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life-cycle, or which are included in the certificate;

(c) provide reasonably accessible means which enable a relying party to ascertain from the certificate:

(i) the identity of the certification service provider;

(ii) that the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;

(iii) that signature creation data were valid at or before the time when the certificate was issued;

(d) provide reasonably accessible means which enable a relying party to ascertain, where relevant, from the certificate or otherwise:

(i) the method used to identify the signatory;

(ii) any limitation on the purpose or value for which the signature creation data or the certificate may be used;

(iii) that the signature creation data are valid and have not been compromised;

(iv) any limitation on the scope or extent of liability stipulated by the certification service provider;

(v) whether means exist for the signatory to give notice pursuant to article 8(1)(b);

(vi) whether a timely revocation service is offered;

(e) where services under paragraph (d)(v) are offered, provide a means for a signatory to give notice pursuant to article 8 (1)(b) and, where services under paragraph d(vi) are offered, ensure the availability of a timely revocation service;
(f) utilize trustworthy systems, procedures and human resources in performing its services.

(2) A certification service provider shall be liable for its failure to satisfy the requirements of paragraph (1).

Article 10. Trustworthiness

For the purposes of article (9)(1)(f), in determining whether, or to what extent, any systems, procedures and human resources utilized by a certification service provider are trustworthy, regard may be had to the following factors:
(a) financial and human resources, including existence of assets;
(b) quality of hardware and software systems;
(c) procedures for processing of certificates and applications for certificates and retention of records;
(d) availability of information to signatories identified in certificates and to potential relying parties;
(e) regularity and extent of audit by an independent body;
(f) the existence of a declaration by the State, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing; or
(g) any other relevant factor.

Article 11. Conduct of the relying party

A relying party shall bear the legal consequences of its 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; and
    (ii) observe any limitation with respect to the certificate.

Article 12. Recognition of foreign certificates and electronic signatures

(1) In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had to:
(a) the geographic location where the certificate is issued or the electronic signature created or used; or

(b) the geographic location of the place of business of the issuer or signatory.

(2) A certificate issued outside [*the enacting State*] shall have the same legal effect in [*the enacting State*] as a certificate issued in [*the enacting State*] if it offers a substantially equivalent level of reliability.

(3) An electronic signature created or used outside [*the enacting State*] shall have the same legal effect in [*the enacting State*] as an electronic signature created or used in [*the enacting State*] if it offers a substantially equivalent level of reliability.

(4) In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of paragraphs (2) or (3), regard shall be had to recognized international standards and to any other relevant factors.

(5) Where, notwithstanding paragraphs (2), (3) and (4), parties agree, as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law.

APPENDIX C

Excerpt from the Code of Banking Practice

2nd Edition, November 1996

5. CARDS/PINS/PASSWORDS

5.1 Issuing cards/pins/passwords

5.1.1 We will issue cards, PINs or passwords (other than replacements) only on instruction from the customers on whose accounts they are to be issued.

5.1.2 Where cards, PINs or passwords are issued to you personally, we must be satisfied about your identity before allowing cards to be used, and will, where possible, obtain signed acknowledgement of receipt from you. Where cards, PINs or passwords are not issued personally, the cards will be issued separately from the PINs or passwords.

5.1.3 You will not be liable for losses occurring before you receive your cards or, if applicable, your PINs or passwords. In any dispute about receipts of cards, PINs or passwords that are not issued to you in person, we will not rely only on proof of despatch to your correct address as proof that the cards, PINs or passwords were received.

5.1.4 We will inform you whether cards issued have more than one function, and if so, what the functions are and what options are available to you. We will comply with requests from you not to issue PINs where you do not wish to use the functions operated by a PIN.

5.1.5 We will inform you in our terms and conditions of daily cash withdrawal limits applying to cards or other electronic banking services.

5.1.6 We will inform you of any variation to current terms and conditions applying to a card, PIN or password, and will give at least 14 days notice of any variation of terms and conditions, except for interest rate and other variations that are subject to market fluctuations.

5.1.7 Any changes applicable to cards, PINs or passwords that we are free to make unilaterally will be notified in the same way as provided in paragraph 3.6 of this Code.

5.2 Using cards

5.2.1 We will inform you that you cannot stop transactions initiated by cards.

5.2.2 We will also inform you of the risks involved if card transactions are authorised in advance of the receipt of goods or services.

5.2.3 When printed transaction records are offered or produced, they will include:

(i) the amount of the transaction;

(ii) the date and, if practicable, the time of the transaction;

(iii) the type of transaction; for example, deposit, withdrawal, transfer, or purchase;

(iv) data that enables us to identify the cardholder and the transaction;

(v) a name, number or code that identifies the location where the transaction was made;

(vi) where relevant, the name of the person or account to whom the payment or deposit was made;

(vii) in the case of accounts accessed at an ATM, the balance of the account, where possible; and

(viii) for an electronic debit card transaction, non-specific information to enable you, but no unauthorised person, to identify the account(s) being debited and/or credited.

5.3 Security of cards/pins/passwords

5.3.1 When PINs or passwords are issued or selected, we will inform you that PINs or passwords are individually allocated to each customer and, to prevent loss or theft, should not be written down. Cards that are lost or stolen together with the PINs or passwords can be used by others for unauthorised transaction, which may result in loss.

5.3.2 We will inform you of the importance of, and your responsibility for, safeguarding cards and committing PINs or passwords to memory. Explicit warning will also be given against:

(i) keeping any record of PINs or passwords. If you have difficulty remembering your PIN or password, you should consult your bank for advice on PIN or password selection;

(ii) writing PINs or passwords on cards or anywhere else;

(iii) negligent care of cards and disclosure of PINs or passwords by, for example, failing to take reasonable care when keying-in PINs at terminals to prevent others from identifying them;

(iv) disclosing PINs or passwords to any other person, including family members or those in apparent authority, including bank staff; and

(v) the risks of disclosing card numbers and expiry dates in advance of receipt of the goods or services ordered.

5.3.3 In cases of illness or disability, by agreements with your bank, an additional card may be issued to a nominated person authorised by the account holder. The account holder will remain liable for all transactions arising from use of that card.

5.3.4 You will not select PINs that we advise are unsuitable, such as birth dates, sequential numbers (eg 3456), parts of personal telephone numbers and other easily accessible personal data, or number combinations that may be easily identified (eg 1111).

5.3.5 You will not select passwords that we advise are unsuitable, such as family or street names, or birth months.

5.3.6 You will conform to internationally accepted standards for methods of generation, storage and terminal security relating to PINs and passwords, to ensure confidentiality and security for your protection.

5.3.7 We will encourage third parties to maximise your PIN and password security. For EFT facilities on our own premises, we will ensure that new and replacement equipment are of a type that maximises your PIN and password security.

5.4 Reporting loss or theft

5.4.1 You are responsible for promptly advising your bank of the loss or theft of cards, unauthorised use of cards, or actual or possible disclosure to other persons of your PINs or passwords as soon as

this becomes known to you. We will log such reports, so that there are records showing when notifications were made.

5.4.2 We will provide and publicise domestic toll-free telephone numbers so that you can report the loss or theft of cards, unauthorised use of cards, or disclosure of PINs or passwords as soon as this becomes known. Should such facilities be temporarily unavailable, we will be liable for any actual card transaction losses due to non-notification, provided we are notified within a reasonable time after the service is restored.

5.4.3 We will inform you, on request, of the procedures you must use to report disputed transactions or the loss or theft of cards when you are travelling overseas.

5.5 Customer liability

5.5.1 You are not liable for loss caused by:

(i) fraudulent or negligent conduct by employees or agents of a bank or parties involved in the provision of electronic banking services;

(ii) faults that occur in the machines, cards or systems used, unless the faults are obvious or advised by message or notice on display;

(iii) unauthorised transactions occurring before you have received your cards, PINs or passwords (see paragraph 5.1.3 above); and

(iv) any other unauthorised transactions where it is clear that you could not have contributed to the loss.

5.5.2 You are liable for all loss if you have acted fraudulently, either alone or together with any other person.

5.5.3 You may be liable for some or all loss from unauthorised transactions if you have contributed to or caused that loss by, for example:

(i) selecting unsuitable PINs or passwords (see paragraphs 5.3.4 and 5.3.5);

(ii) failing to reasonably safeguard cards;

(iii) keeping written records of PINs or passwords;

(iv) parting with cards and/or disclosing PINs or passwords to any other person;

(v) failing to take all reasonable steps to prevent disclosure to any other person when keying-in PINs or using passwords; or

(vi) unreasonably delaying notification to your bank of the loss or theft of cards, or of the actual or possible disclosure to any other person of PINs or passwords (see paragraph 5.4.1).

5.5.4 If you have promptly reported the loss or theft of cards or the actual or possible disclosure of PINs or passwords, you are not liable for loss occurring after notification, unless you have acted fraudulently or negligently.

5.5.5 If you have not acted fraudulently or negligently and have not contributed to or caused losses from unauthorised use, your liability for any loss occurring before notification to your bank or, if you are overseas, to any agent of your bank, is limited to the lesser of:

(i) $50, or such sum as your bank's terms and conditions of use may specify;

(ii) the balance of your account(s), including any pre-arranged credit; or

(iii) the actual loss at the time you notify your bank.

This limitation of your liability may not apply to stored value cards or the stored value function of a multi-function card.

5.5.6 If you have not acted fraudulently or negligently but have contributed to or caused losses from unauthorised transactions, you may be liable for some or all of the actual losses occurring before notification to your bank except for:

(i) that portion of the total losses incurred on any other day that exceeds the transaction limit applicable to your card or account(s); or

(ii) that portion of the total losses incurred that exceeds the balance of your account(s), including any prearranged credit.

5.5.7 We will not avoid liability to you for direct losses caused by an EFT transaction only by reason of the fact that we are a party to a shared EFT system.

5.5.8 Individual banks may have their own terms and conditions applying to the issue, use, security and liability for cards, PINs and passwords, and for losses. These terms and conditions may be additional to, but must not be inconsistent with the provisions of this Code.

APPENDIX D

Other legislation based on the UNCITRAL Model Law on Electronic Commerce

AUSTRALIA

THE AUSTRALIAN FEDERAL PARLIAMENT passed the Electronic Transactions Act in November 1999 and it came into force on 15 March 2000. The Act has a two-step implementation process. Prior to 1 July 2001 it will apply only to laws of the Commonwealth specified in the Regulations. After that date it will apply to all laws of the Commonwealth unless specifically excluded. The first set of Electronic Transactions Regulations have been made and are now in operation. The Act can be viewed at <http://www.austlii.edu.au/au/legis/cth/consol_act/eta1999256/>.

CANADA

The Uniform Law Conference of Canada, which promotes the harmonisation of Canadian legislation, produced a Uniform Electronic Commerce Act (UECA) based on the Model Law. The UECA has been enacted in various forms in Ontario, Saskatchewan, Nova Scotia and Manitoba, and Bills based on the UECA have been introduced in British Columbia, the Yukon and Quebec. The UECA can be viewed at <http://www.law.ualberta.ca/alri/ulc/current/euecafin.htm>.

In addition the Personal Information and Electronic Documents Act 2000 contains provisions regarding legal requirements in respect of electronic documents. It applies to federal statutes and regulations only. The Act received Royal Assent on 13 April 2000, but is not yet in force. Part 2 came into force 1 May 2000 but applies only to designated provisions of law, and none have yet been designated.

EUROPEAN UNION

Directive 1999/93/EC (OJ L013 19.01.2000, 12) relates to a Community framework for electronic signatures and can be viewed at <http://europa.eu.int/eur-lex/en/lif/dat/1999/en_399L0093.html>. The purpose of the Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain certification services.

Directive 2000/31/EC (OJ L178 17.07.2000, 1) relates to "certain legal aspects of information society services, in particular electronic commerce, in the Internal Market". It can be viewed at <http://europa.eu.int/eur-lex/en/lif/dat/2000/en_300L0031.html>. The Directive approximates certain national provisions on what are termed "information society services", relating to the internal market, the establishment of service providers, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct, out-of-court dispute settlements, court actions and co-operation between member States. Paragraph 58 of the Preamble to the Directive states that, in view of the global dimension of electronic commerce, it is appropriate to ensure that the Community rules are consistent with international rules, and that the Directive is without prejudice to the results of discussions on legal issues within international organisations, including UNCITRAL.

INDIA

The Indian Government is currently consulting on two draft Acts (the Electronic Commerce Act and the Electronic Commerce Support Act) which have been prepared to facilitate a secure regulatory environment for Electronic Commerce. The Indian Law Ministry is working on amalgamating the draft Acts into a single statute. The Electronic Commerce Act incorporates the Model Law and establishes a regime for "secure electronic signatures" which is influenced by the Singapore and Illinois legislation (discussed in ECom 1, appendix E). The Act also creates some criminal offences relating to computer records and the use of computers. Sources for the Act's provisions include the American Bar Association Digital Signature Guidelines and various United States Penal Codes, as well as the Model Law. To view the draft Acts visit <http://commin.nic.in/doc/ecact.htm>.

UNITED KINGDOM

The Electronic Communications Act 2000 received Royal Assent on 22 May 2000. Its purpose is stated to be to facilitate the use of electronic communications and electronic data storage; to make provision about the modification of licences granted under section 7 of the Telecommunications Act 1984; and for connected purposes. The Act implements certain provisions of the EU Electronic Signatures Directive (1999/93/EC), which is intended to facilitate the use of electronic signatures and to contribute to their legal recognition throughout the European Union. The Explanatory Note to the Act states that it is also compatible with UNCITRAL's Model Law on Electronic Commerce and draft Model Law on Electronic Signatures. The Act can be viewed at <http://www.hmso.gov.uk/acts/acts2000/20000007.htm#16>.

UNITED STATES

The Uniform Laws Commissioners completed the Uniform Electronic Transactions Act (UETA) in 1999. The UETA has been enacted in 22 states, and is currently before the legislatures of six further states. The UETA is intended to support the use of electronic commerce and its purpose is stated as being to establish the legal equivalence of electronic records and signatures with paper writings and manually-signed signatures, removing barriers to electronic commerce. It can be viewed at <http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm>.

Select bibliography

REPORTS

New Zealand Law Commission *Electronic Commerce Part 1: A Guide for the Legal and Business Community: NZLC R50* (Wellington, 1998)

New Zealand Law Commission *Cross-Border Insolvency: Should New Zealand Adopt the UNCITRAL Model Law on Cross-Border Insolvency: NZLC R52* (Wellington, 1999)

New Zealand Law Commission *Computer Misuse: NZLC R54* (Wellington, 1999)

New Zealand Law Commission *Evidence: NZLC R55* (Wellington, 1999)

New Zealand Law Commission *Electronic Commerce Part 2: A Basic Legal Framework: NZLC R58* (Wellington, 1999)

New Zealand Law Commission *International Trade Conventions: NZLC SP5* (Wellington, 2000)

Office of the Privacy Commissioner *Necessary and Desirable: Privacy Act 1993 Review: Report of the Privacy Commissioner* (Wellington, 1998)

United Nations Congress, *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, A/CONF.187/L.10, report of Committee II (Workshop on Crimes Related to the Computer Network), Vienna, April 2000

Office of the Banking Ombudsman's Annual Report 1996–1997.

Office of the Banking Ombudsman's Annual Report 1998–1999.

Office of the Banking Ombudsman's Annual Report Case Note Compendium.

UNICITRAL Working Group on Electronic Commerce, 32nd session (May–June 1999) A/54/17

UNICTRAL Working Group on Electronic Commerce, 33rd session (September 2000) A/55/17

TEXTS

D Goddard *The Laws of New Zealand: Conflict of Laws: Jursidiction and Foreign Judgments* (Butterworths, Wellington, 1996)

ARTICLES AND PAPERS

L Determann "The New German Internet Law" (1998) 22 Hastings International and Comparative Law Review 113

"Cyber crime treaty raises concern" *The Dominion*, Wellington, New Zealand, 30 June 2000

P Heath "An International Approach to Computer Crime" (2000) UNCITRAL and the Developing International Law of Electronic Commerce, New York, 24 February 2000; published Documentary Credit World 34 (June 2000, Vol 4 No 6)

JC Rodriguiz "A Comparative Study of Internet Content Regulations in the United States and Singapore: The Invincibility of Cyberporn" (2000) 1 Asian-Pacific Law and Policy Journal 9

BJ Waldman "A Unified Approach to Cyber-Libel: Defamation on the Internet, a Suggested Approach" (1999) 6 Richmond Journal of Law and Technology 9

CASES

ACLU v Reno No 91-CV-5591, (ED Pa 2/1/99)

American Library Assoc. v US Department of Justice (1996) 929 F Supp 824

Bilgola Enterprises Ltd & Ors v Dymocks Franchise Systems (NSW) Pty Ltd [2000] 3 NZLR 169 (CA)

Blumenthal v Drudge and America Online (1998) 992 F Supp 44 (DDC)

Erven Warnink BV v J Townend & Sons [1979] AC 731, 743

Jardine Risk Consultants Limited v Beal (29 June 2000) unreported, Court of Appeal, CA 208/99

R v Wilkinson [1999] 1 NZLR 403

Reno v ACLU 117 S.Ct. 2329, 521 US 844, 138

Stratton Oakmont v Prodigy Services 23 Media L Rep (BNA) 1794 (NY Sup Ct May 24, 1995)

OTHER LAW COMMISSION PUBLICATIONS

Report series

NZLC R1	Imperial Legislation in Force in New Zealand (1987)
NZLC R2	Annual Reports for the years ended 31 March 1986 and 31 March 1987 (1987)
NZLC R3	The Accident Compensation Scheme (Interim Report on Aspects of Funding) (1987)
NZLC R4	Personal Injury: Prevention and Recovery (Report on the Accident Compensation Scheme) (1988)
NZLC R5	Annual Report 1988 (1988)
NZLC R6	Limitation Defences in Civil Proceedings (1988)
NZLC R7	The Structure of the Courts (1989)
NZLC R8	A Personal Property Securities Act for New Zealand (1989)
NZLC R9	Company Law: Reform and Restatement (1989)
NZLC R10	Annual Report 1989 (1989)
NZLC R11	Legislation and its Interpretation: Statutory Publications Bill (1989)
NZLC R12	First Report on Emergencies: Use of the Armed Forces (1990)
NZLC R13	Intellectual Property: The Context for Reform (1990)
NZLC R14	Criminal Procedure: Part One: Disclosure and Committal (1990)
NZLC R15	Annual Report 1990 (1990)
NZLC R16	Company Law Reform: Transition and Revision (1990)
NZLC R17(S)	A New Interpretation Act: To Avoid "Prolixity and Tautology" (1990) (and Summary Version)
NZLC R18	Aspects of Damages: Employment Contracts and the Rule in *Addis v Gramophone Co* (1991)
NZLC R19	Aspects of Damages: The Rules in *Bain v Fothergill* and *Joyner v Weeks* (1991)
NZLC R20	Arbitration (1991)
NZLC R21	Annual Report 1991 (1991)
NZLC R22	Final Report on Emergencies (1991)
NZLC R23	The United Nations Convention on Contracts for the International Sale of Goods: New Zealand's Proposed Acceptance (1992)
NZLC R24	Report for the period l April 1991 to 30 June 1992 (1992)
NZLC R25	Contract Statutes Review (1993)
NZLC R26	Report for the year ended 30 June 1993 (1993)
NZLC R27	The Format of Legislation (1993)
NZLC R28	Aspects of Damages: The Award of Interest on Money Claims (1994)
NZLC R29	A New Property Law Act (1994)
NZLC R30	Community Safety: Mental Health and Criminal Justice Issues (1994)
NZLC R31	Police Questioning (1994)
NZLC R32	Annual Report 1994 (1994)
NZLC R33	Annual Report 1995 (1995)
NZLC R34	A New Zealand Guide to International Law and its Sources (1996)
NZLC R35	Legislation Manual: Structure and Style (1996)
NZLC R36	Annual Report 1996 (1996)
NZLC R37	Crown Liability and Judicial Immunity: A response to *Baigent's* case and *Harvey v Derrick* (1997)
NZLC R38	Succession Law: Homicidal Heirs (1997)
NZLC R39	Succession Law: A Succession (Adjustment) Act (1997)

NZLC R40	Review of the Official Information Act 1982 (1997)
NZLC R41	Succession Law: A Succession (Wills) Act (1997)
NZLC R42	Evidence Law: Witness Anonymity (1997)
NZLC R43	Annual Report 1997 (1997)
NZLC R44	Habeas Corpus: Procedure (1997)
NZLC R45	The Treaty Making Process: Reform and the Role of Parliament (1997)
NZLC R46	Some Insurance Law Problems (1998)
NZLC R47	Apportionment of Civil Liability (1998)
NZLC R48	Annual Report (1998)
NZLC R49	Compensating the Wrongly Convicted (1998)
NZLC R50	Electronic Commerce Part One: A Guide for the Legal and Business Community (1998)
NZLC R51	Dishonestly Procuring Valuable Benefits (1998)
NZLC R52	Cross-Border Insolvency: Should New Zealand adopt the UNCITRAL Model Law on Cross-Border Insolvency? (1999)
NZLC R53	Justice: The Experiences of Māori Women Te Tikanga o te Ture: Te Mātauranga o ngā Wāhine Māori e pa ana ki tēnei (1999)
NZLC R54	Computer Misuse (1999)
NZLC R55	Evidence (1999)
NZLC R56	Annual Report (1999)
NZLC R57	Retirement Villages (1999)
NZLC R58	Electronic Commerce Part Two: A Basic Legal Framework (1999)
NZLC R59	Shared Ownership of Land (1999)
NZLC R60	Costs in Criminal Cases (2000)
NZLC R61	Tidying the Limitation Act (2000)
NZLC R62	Coroners (2000)
NZLC R63	Annual Report 2000 (2000)
NZLC R64	Defaming Politicians: A Response to *Lange v Atkinson*
NZLC R65	Adoption and Its Alternatives: A Different Approach and a New Framework (2000)
NZLC R66	Criminal Prosecution (2000)
NZLC R67	Tax and Privilege: Legal Professional Privilege and the Commissioner of Inland Revenue's Powers to Obtain Information (2000)

Study Paper series

NZLC SP1	Women's Access to Legal Services (1999)
NZLC SP2	Priority Debts in the Distribution of Insolvent Estates: An Advisory Report to the Ministry of Commerce (1999)
NZLC SP3	Protecting Construction Contractors (1999)
NZLC SP4	Recognising Same-Sex Relationships (1999)
NZLC SP5	International Trade Conventions (2000)

Preliminary Paper series

NZLC PP1	Legislation and its Interpretation: The Acts Interpretation Act 1924 and Related Legislation (discussion paper and questionnaire) (1987)
NZLC PP2	The Accident Compensation Scheme (discussion paper) (1987)
NZLC PP3	The Limitation Act 1950 (discussion paper) (1987)
NZLC PP4	The Structure of the Courts (discussion paper) (1987)

NZLC PP5	Company Law (discussion paper) (1987)
NZLC PP6	Reform of Personal Property Security Law (report by Prof JH Farrar and MA O'Regan) (1988)
NZLC PP7	Arbitration (discussion paper) (1988)
NZLC PP8	Legislation and its Interpretation (discussion and seminar papers) (1988)
NZLC PP9	The Treaty of Waitangi and Māori Fisheries – Mataitai: Nga Tikanga Māori me te Tiriti o Waitangi (background paper) (1989)
NZLC PP10	Hearsay Evidence (options paper) (1989)
NZLC PP11	"Unfair" Contracts (discussion paper) (1990)
NZLC PP12	The Prosecution of Offences (issues paper) (1990)
NZLC PP13	Evidence Law: Principles for Reform (discussion paper) (1991)
NZLC PP14	Evidence Law: Codification (discussion paper) (1991)
NZLC PP15	Evidence Law: Hearsay (discussion paper) (1991)
NZLC PP16	The Property Law Act 1952 (discussion paper) (1991)
NZLC PP17	Aspects of Damages: Interest on Debt and Damages (discussion paper) (1991)
NZLC PP18	Evidence Law: Expert Evidence and Opinion Evidence (discussion paper) (1991)
NZLC PP19	Apportionment of Civil Liability (discussion paper) (1992)
NZLC PP20	Tenure and Estates in Land (discussion paper) (1992)
NZLC PP21	Criminal Evidence: Police Questioning (discussion paper) (1992)
NZLC PP22	Evidence Law: Documentary Evidence and Judicial Notice (discussion paper) (1994)
NZLC PP23	Evidence Law: Privilege (discussion paper) (1994)
NZLC PP24	Succession Law: Testamentary Claims (discussion paper) (1996)
NZLC PP25	The Privilege Against Self-Incrimination (discussion paper) (1996)
NZLC PP26	The Evidence of Children and Other Vulnerable Witnesses (discussion paper) (1996)
NZLC PP27	Evidence Law: Character and Credibility (discussion paper) (1997)
NZLC PP28	Criminal Prosecution (discussion paper) (1997)
NZLC PP29	Witness Anonymity (discussion paper) (1997)
NZLC PP30	Repeal of the Contracts Enforcement Act 1956 (discussion paper) (1998)
NZLC PP31	Compensation for Wrongful Conviction or Prosecution (discussion paper) (1998)
NZLC PP32	Juries in Criminal Trials: Part One (discussion paper) (1998)
NZLC PP33	Defaming Politicians: A response to *Lange v Atkinson* (discussion paper) (1998)
NZLC PP34	Retirement Villages (discussion paper) (1998)
NZLC PP35	Shared Ownership of Land (discussion paper) (1999)
NZLC PP36	Coroners: A Review (discussion paper) (1999)
NZLC PP37	Juries in Criminal Trials: Part Two (discussion paper) (1999)
NZLC PP38	Adoption: Options for Reform (discussion paper) (1999)
NZLC PP39	Limitation of Civil Actions (discussion paper) (2000)
NZLC PP40	Misuse of Enduring Powers of Attorney (discussion paper) (2000)
NZLC PP41	Battered Defendants: Victims of Domestic Violence Who Offend (discussion paper) (2000)
NZLC PP42	Acquittal Following Perversion of the Course of Justice: A Response to *R v Moore* (discussion paper) (2000)
NZLC PP43	Subsidising Litigation (discussion paper) (2000)