E 31AR

LAW·COMMISSION
TE·AKA·MATUA·O·TE·TURE

*Report 58*

# Electronic Commerce Part Two

## A basic legal framework

*November 1999*
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, 1999
ISSN 0113–2334 ISBN 1–877187–45–3
This report may be cited as: NZLC R58
Also published as Parliamentary Paper E 31AR

# Summary of contents

# Contents

*17 November 1999*

Dear Minister

I am pleased to submit to you Report 58 of the Law Commission, *Electronic Commerce Part Two: A basic legal framework*.

Yours sincerely

*The Hon Justice Baragwanath*
President

*The Hon Tony Ryall MP*
Minister of Justice
Parliament Buildings
Wellington

# Preface

OVER THE PAST TWO YEARS the Law Commission has been examining various aspects of the law affected by electronic commerce. Our work seeks to ascertain whether any changes to the law are needed to fit the electronic environment in which much business is now carried out.

From the civil law perspective, the Commission started a new project in October 1997 which culminated in the publication, on 1 October 1998, of *Electronic Commerce Part One: A Guide for the Legal and Business Community* (NZLC R50) (ECom 1). From the criminal law perspective, two reports have been published. The first recommended an amendment to the Crimes Act 1961 to address a specific problem exposed by the judgment of the Court of Appeal in *R v Wilkinson*.[1] The second report dealt more generally with the issue of computer misuse in New Zealand and the need for criminal legislation.[2] We discuss some aspects of the *Computer Misuse* report in chapter 12 and touch on the interrelationship between the criminal law and the law of torts in chapter 13.[3]

After the Commission's release of ECom 1 in October last year, the Ministry of Commerce published a paper emphasising the importance of the "knowledge economy" to New Zealand as we approach the twenty-first century: *Electronic Commerce: The Freezer Ship of the 21st Century*.[4] Following release of that paper, the Government established an Electronic Commerce Steering Com-

---

1 [1999] 1 NZLR 403 and *Dishonestly Procuring Valuable Benefits: NZLC R51* (Wellington 1998). The question was whether the crime of theft could be committed when funds were transferred electronically. The court held that such a transfer of funds was a chose in action not caught by the expression "capable of being stolen" in s 217 of the Crimes Act 1961. In September 1999 the Crimes Amendment Bill (No 6) had its first reading in Parliament. It is intended that the Bill will remove the problem highlighted in *R v Wilkinson* and *Dishonestly Procuring Valuable Benefits* as it removes the concept of "things capable of being stolen".

2 *Computer Misuse: NZLC R54* (Wellington 1999).

3 Para 235.

4 Ministry of Commerce, November 1998.

mittee (the Steering Committee) to advise it on various issues affecting electronic commerce.[5] The Law Commission is represented on that Steering Committee. Beneath the Steering Committee is a structure of Sector Committees designed to coordinate work being done in the public sector, and to feed relevant information through to the Steering Committee. In appendix A we set out the structure and membership of these committees. The Steering Committee reports directly to the Minister for Information Technology. The Commission has also consulted on questions of policy with the Steering Committee. The Steering Committee has expressed broad agreement with the Commission's policy as formulated in this report.

We raised a number of questions for submission in ECom 1. We have received many helpful submissions from both the public and the private sectors. This report responds to those questions. In general we received wide support in submissions for the views expressed in ECom 1. We did however receive some criticism for taking what was perceived to be an over-simplistic approach to our analysis of how the domestic law affected electronic commerce. There is some truth in the suggestion that our analysis of existing law was elementary in nature. But we never aimed to write a textbook of discrete legal topics; rather, we intended to apply well settled principles of law to the electronic environment to ascertain whether adaptation or reform of the law was needed. We adopt the same style in this report.

In this report we make recommendations for enactment of a basic legal framework in New Zealand which will remove core problems arising from the use of electronically generated information and identify further issues on which submissions are sought. A summary of our proposals is contained in chapter 19.[6] A summary of further questions upon which we seek submissions is listed at pages xxii–xxiii. We recommend a basic statutory framework at this stage because many of the issues identified in this report are truly international in nature and solutions to them will be distilled from work still being done in various international forums. The reasons why we believe a basic statutory framework is required are set out in chapter 2.

---

5 The Steering Committee comprises representatives of the Ministry of Commerce, Ministry of Foreign Affairs and Trade, Law Commission, Ministry of Consumer Affairs, Department of Prime Minister and Cabinet, Inland Revenue Department and the Treasury.

6 Paras 332–341.

Much of our work has focused on developments at an international level. The Commission is pleased that New Zealand is now being represented at international forums considering, amongst other things, electronic commerce issues. Such representation ensures that we have an opportunity to shape the form, and to be heard on the content, of the Model Laws or Conventions which may ultimately be adopted by individual States. For example, New Zealand was represented at the February 1999 and September 1999 sessions of the United Nations Commission on International Trade Law's (UNCITRAL) *Working Group on Electronic Commerce* (which is currently dealing with issues involving electronic signatures) and at the June 1999 meeting of the *Hague Conference on Private International Law*.[7] Officials from the Ministry of Foreign Affairs and Trade, Ministry of Commerce and other government agencies continue to represent New Zealand at forums such as APEC (Asia Pacific Economic Cooperation) and OECD (Organisation for Economic Cooperation and Development) both of which have electronic commerce on their agendas. Indeed, some impetus to discussions on electronic commerce within APEC and OECD was given by speeches made in late 1998 at OECD (Ottawa) and APEC (Kuala Lumpur) meetings by the President of this Commission, Hon Justice Baragwanath.[8] Recently, the President addressed an APEC/World Trade Centre (WTC) meeting in Auckland.[9]

To assist it in the preparation of this report, the Law Commission established an Electronic Commerce Advisory Committee (the Advisory Committee). 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 expresses its gratitude

---

7 Paul Heath QC, of this Commission, represented New Zealand at the UNCITRAL Working Group in Vienna while David Goddard, Barrister, Wellington, represented New Zealand at the Hague Conference.

8 See Hon Justice Baragwanath "A Call for Joint Action to Make Changes in International and Domestic Law which are Critical to a Borderless World of Electronic Commerce" (address to APEC Conference, Kuala Lumpur, 21 October 1998); available at http://www.lawcom.govt.nz/speeches/apececom211098.htm.

9 Hon Justice Baragwanath, "Changes in International and Domestic Law which are Critical to a Borderless World of Electronic Commerce" (address to APEC Conference, Auckland, 6 September 1999); available at <http://www.lawcom.govt.nz/speech_index.html>.

to members of the Advisory Committee for their assistance in the preparation of this report. It is fair to say, however, that our position on some issues does not reflect the views of all of the members of the Advisory Committee.

While the assistance of both our Advisory Committee and the Steering Committee in developing issues of policy is much appreciated, the responsibility for recommendations made rests with this Commission alone.

We are also grateful to a number of people for making submissions and providing information to us. A list of persons who made submissions on ECom 1 appears at page xxiv. A list of those to whom we express a particular acknowledgement of assistance is set out at page xv.

This report is available not only in hard copy, but also through our website: www.lawcom.govt.nz.

The Commissioner in charge of the preparation of this report is Paul Heath QC. The research for the report has been undertaken by Megan Leaf, Jason Clapham and Lucy McGrath to whom the Commission expresses its appreciation.

Submissions on remaining questions should be addressed to Megan Leaf at the Law Commission. Submissions can be sent by email to MLeaf@lawcom.govt.nz. We ask that submissions be made to us on or before 30 June 2000. A third report will be issued in late 2000 addressing remaining issues.

---

# Acknowledgements

Christopher Darlow, Grove Darlow & Partners, Barristers and Solicitors, Auckland

Christopher Nicoll, Senior Lecturer in Commercial Law, University of Auckland

Colin Minihan, Principal Legal Officer, Security Law and Justice Branch, Information and Security Law Division, Attorney-General's Department, Canberra, Australia

David Goddard, Barrister, Wellington

Dr Gerold Herrmann, Secretary, United Nations Commission on International Trade Law (UNCITRAL)

Dr Henry Wolfe, Senior Lecturer of the Information Science Department, University of Otago, Dunedin

Elizabeth Longworth, Barrister and Solicitor, Auckland

Jim Higgins, Managing Director, The Networking Edge Limited, Wellington

John Gregory, General Counsel, Policy Branch, Ministry of the Attorney-General (Ontario), Canada

Michael Wigley, Barrister & Solicitor, Wellington

Office of the Privacy Commissioner

Paul David, Partner, Russell McVeagh McKenzie Bartleet and Co, Auckland

Professor Mark Sneddon, Melbourne University, Special Counsel on Electronic Commerce, Clayton Utz, Solicitors, Melbourne, Australia

Robert Howland, Winchester, England

Members of the government Electronic Commerce Steering Committee:

– Ministry of Commerce

– Ministry of Foreign Affairs and Trade

– Ministry of Consumer Affairs
– Department of Prime Minister and Cabinet
– Inland Revenue Department
– the Treasury.

---

# Executive summary

E1 THE TRANSACTION OF BUSINESS through electronic means is growing rapidly. There is public interest in facilitating that type of trade (in this report, termed electronic commerce). Unless there are good reasons to the contrary, it seems clear that legal impediments to electronic commerce should be removed.

E2 In determining whether it is necessary to enact legislation to remove barriers to electronic commerce we have applied the four guiding principles identified in ECom 1. Those principles are:

- The right to choose whether to do business through the use of paper documentation or by electronic means without avoidable uncertainty arising out of the use of electronic means of communication (the *choice* principle).
- Ensuring that the fundamental principles underlying the law of contract and tort remain untouched save to the extent that adaptation is required to meet the needs of electronic commerce (the *adaptation* principle).
- Expression of any laws enacted to adapt the law of contract or the law of torts to the use of electronic commerce in a technologically neutral manner (the *technological neutrality* principle).
- Compatibility between principles of domestic and private international law as applied in New Zealand and those applied by our major trading partners (the *compatibility* principle).

E3 All of those principles rest on the functional equivalence principle on which the UNCITRAL Model Law on Electronic Commerce (the Model Law) is based. Submissions made to us in response to ECom 1 emphasised a further principle: private sector leadership. It is suggested that the private sector should lead development in this area and that the Government's role should be confined to the removal of barriers to electronic commerce and to the general facilitation of trade which is carried on through electronic means. We adopt that principle as a fifth principle in relation to the facilitation of electronic commerce. Adoption of this principle is wholly consistent with the emphasis on party autonomy to be found

in article 4 of the Model Law and with the desirability of employing contractual solutions in preference to those imposed by legislation. But, equally, it does not displace the need for the State to enact appropriate consumer protection laws.

E4 The Commission recommends enactment of an Electronic Transactions Act along similar lines to the Electronic Transactions Bill currently before the Federal Parliament in Australia (the Australian Bill). Our reasons for recommending statutory intervention are set out in chapter 2. 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.

E5 It is important that, so far as practicable, New Zealand's Electronic Transactions Act should accord with the Australian version to reduce (if not completely minimise) conflict of laws problems when trans-Tasman trade is involved.[10] It would also have the advantage of general consistency. In general terms our proposed statute would adopt articles 4 (Party autonomy), 5 (Non-discrimination), 5 bis (Incorporation by reference), 6 (Writing), 7 (Signature), 10 (Retention of electronically generated messages) and 15 (Time and place of dispatch and receipt of electronically generated documents) of the Model Law. For reasons given later in this report it is proposed to defer consideration of remaining issues involving electronic signatures,[11] allocation of risk through default rules dealing with attribution of messages (article 13 of the Model Law)[12] and provisions of the Model Law dealing with transportation documentation (articles 16 and 17 of the Model Law) until further work being carried out in international forums has matured. The Commission proposes to publish a third electronic commerce report in late 2000 which will address these issues and make recommendations as to whether any additions are needed to the basic legal framework which we now recommend. The deadline for submissions on this report has been extended considerably so that progress of that work will be available to those who wish to make submissions.

---

[10] Generally, see chapter 14, Conflict of Laws.

[11] See chapter 9, Electronic Signatures, para 152.

[12] See chapter 3, Contract, paras 48–52.

E6 We do not recommend that article 14 of the Model Law (which deals with acknowledgement of receipt)[13] should be adopted for reasons detailed at paragraphs 60–61.

E7 Articles 8 and 9 of the Model Law deal primarily with evidential issues.[14] On 24 August 1999 the Commission published its final report on its Evidence reference: *Evidence: Reform of the Law* (NZLC R55). We recommend that the Evidence Code set out in the second volume to that report be enacted at the same time as the Electronic Transactions Act – to remove all barriers of an evidential nature. We set out the reasons why we believe the Evidence Code is sufficient to remove all barriers in chapter 7.[15]

E8 The mandate of UNCITRAL is to consider international trade law issues; the Model Law states that it is not intended to override any rule of law intended for the protection of consumers.[16] Work is still being done on consumer issues at OECD. New Zealand is being represented at OECD by the Ministry of Consumer Affairs. It may be necessary to revisit certain consumer protection issues in our next report.[17] But, in the meantime, we recommend that our proposed Electronic Transactions Act apply to all consumer transactions conducted "in trade".[18]

E9 Remaining parts of this report focus debate on options for reform as a result of submissions made to us on ECom 1 and as a result of debate which has occurred since publication of that report. This is particularly true of the law of torts,[19] conflict of laws,[20] electronic signatures[21] and questions of attribution.[22] Some new banking issues are also raised for consideration.[23] Other chapters simply

---

[13] See chapter 3, Contract, paras 59–60.

[14] Article 8 goes beyond evidential issues: see chapter 8, Record Retention. See also our discussion of the Australian Electronic Transactions Bill on this topic, paras 130–132, 136–137.

[15] See generally, chapter 7, Evidence.

[16] Model Law, article 1, footnote **.

[17] See chapter 6, Consumer Issues, para 114.

[18] See chapters 2, The Need for Legislation and 6; para 34 and 107 and n 206.

[19] See chapter 13, The Law of Torts.

[20] See chapter 14, Conflict of Laws.

[21] See chapter 9, Electronic Signatures.

[22] See chapter 3, Contract, paras 48–52.

[23] See chapter 15, Banking, paras 294–312.

inform readers of the government agency responsible for administration of those parts of the law and outline the type of issues which are being addressed by bodies other than the Law Commission.[24] Submissions on these issues should be made directly to the agencies concerned.

E10 In our conclusions,[25] we refer to the need for further work. We propose that the further international work on electronic signatures, conflict of laws and consumer transactions be monitored and followed up by further recommendations to be made in our next electronic commerce report. At that stage it can be decided whether an expanded legal framework is necessary.

E11 We also discuss wider issues; in particular the interrelationship of the criminal law[26] and the law of torts.[27] So far as the criminal law is concerned, we have adopted, with one significant addition, the recommendations made in our *Computer Misuse*[28] report. That addition recommends the creation of a fifth offence and explains the reasons for it.[29] So far as the law of torts is concerned, we have made specific recommendations about Internet Service Providers both generally and in the context of defamation law and have raised a number of further questions for submission.[30]

E12 It is important to stress that our proposed Electronic Transactions Act will not create a perfect world for those who wish to engage in business through electronic means. But, it will create a better environment than currently exists by removing immediate barriers. Other barriers to which our attention has been drawn are equally applicable to the physical world and, hence, unnecessary to deal with in the context of a report restricted to electronic commerce.

E13 For ease of reference, appendix A to this report contains a summary of the structure of the government committees established to consider electronic commerce.[31] Appendix B to this report

---

[24] See chapter 10, Security and Encryption, chapter 11, Privacy, chapter 15, Banking, chapter 16, Securities, chapter 17, Intellectual Property and chapter 18, Taxation.

[25] See chapter 19, Conclusions, paras 332–342.

[26] See chapter 12, Criminal Law, paras 185 and 195.

[27] See chapter 13, The Law of Torts, para 235.

[28] *NZLC R54*, paras 87–94.

[29] Chapter 12, para 192.

[30] Chapter 13, paras 240–270.

[31] Page 142.

replicates the Model Law with its Guide to Enactment. This avoids the need to repeat extensively reasons for and against particular Model Law provisions which are summarised in the Guide. While our text concentrates specifically on the need (or otherwise) for the adoption of Model Law provisions in New Zealand, our comments should be read in conjunction with the Guide to Enactment. Appendix C is a reproduction of the Australian Bill. Appendix D reproduces relevant provisions of the Evidence Code recommended by the Commission in its August 1999 report. Appendix E is a summary of recent overseas legislation concerning electronic signatures.

E14 A summary of questions raised for further debate is set out later in this report.[32] The Commission awaits submissions on those issues.

---

[32] See pages *xxii–xxiii* and para 342.

# Summary of further questions

WE SEEK FURTHER SUBMISSIONS on the following matters which will be addressed in our third report:

- 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 form part of a voluntary industry code?
- In relation to the privacy issues raised by caching:
  - are there any practical problems and issues in the application of the existing law;
  - if so, do those problems arise in relation to collection, holding or giving access; and
  - if a law change is warranted, how that amendment might be framed?
- In general on whether legislation is required to allow the use of electronic transportation documents.
- We are of the view that there is not, as yet, a demonstrable need for legislative intervention to provide greater protection against the misuse of information. However, as there may be a demonstrable need in the near future for added protection, we seek further submissions on:
  - 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 options are suggested to deal with the issues raised?

---

# List of persons who made submissions on ECom 1

Anna Kingsbury, Lecturer, School of Law, University of Waikato

ASB Bank Limited

Baldwin Shelston Waters

Frank Chan

Government Communications Security Bureau

Information and Law Group of the School of Law, University of Waikato

Information Technology Association of New Zealand

Kensington Swan

Mark Perry and Laurette Barnard, Faculty of Law, University of Auckland

Ministry of Commerce

Ministry of Consumer Affairs

New Zealand Bankers' Association

New Zealand Customs Service

New Zealand Post

Reserve Bank of New Zealand

Securities Commission

Susan French, Department of Accountancy and Business Law, Massey University

Telecom New Zealand Limited

The Caldeson Consultancy

The Commercial and Business Law Committee of the New Zealand Law Society

Tim Richards, Solicitor, Rudd Watts & Stone

# 1
# Introduction

## THE FIRST REPORT

1 IN ECOM 1 we noted that no single definition of the term "electronic commerce" had attained universal approval.[33] We said:

> Electronic Commerce is a generic name given to business transactions which are entered into through electronic rather than paper-based means . . . For the purposes of this paper, the term "electronic commerce" means the use of electronic communications technology (instead of paper, telephone or face-to-face meetings) for business purposes in the widest sense. Electronic commerce is not limited to the purchase and sale of goods or services on the internet: rather, it extends to cover a number of primary and support activities which include electronic publishing, intra-organisational communications (eg, through intranets), computer-supported meetings and communications with other businesses. In this paper the word "internet" is used as shorthand for interconnected computer networks; it is not intended to denote any particular form of computer network.

2 We adopt the same approach to electronic commerce in this report. From time to time, we will refer to some more general issues arising out of the use of electronically generated information. Our references to such matters will pertain to the need for a holistic approach by the law to all aspects of electronic technologies, which can assist in the growth of the New Zealand economy. Such an approach necessitates discussion of both civil and criminal law.

3 The benefits of electronic commerce were set out in ECom 1 by reference to Viehland's summary as being:[34]

- lower information transfer costs;
- lower procurement costs;
- reduced inventory costs;
- product customisation;

---

[33] ECom 1, para 1 (footnotes omitted).

[34] ECom 1, para 5.

- the ability to conduct business with distant partners in the same way as with neighbouring partners; and
- increased operational efficiency.

## A BASIC LEGAL FRAMEWORK

4 This report must be read in conjunction with ECom 1. Where legal issues have been discussed in detail in ECom 1 we simply refer back to that discussion rather than repeat it in this report.

5 We recommend that a basic legal framework be established by an overarching Electronic Transactions Act. The Act should be confined to electronic transactions conducted "in trade", as that term is broadly defined by the Fair Trading Act 1986,[35] to avoid the need to list individually many of the legal requirements we wish to exempt from the Act's application. The need for such legislation is discussed in chapter 2. Generally, enactment of our proposed Electronic Transactions Act will facilitate electronic commerce by removing barriers to conducting business in this way.

6 We recognise that in building a legal framework it is necessary to have regard to the international nature of the internet and the ease with which electronically generated transactions can cross borders. In formulating the principles to underpin our proposed Electronic Transactions Act we have, so far as possible, adopted provisions of the Model Law which are based on internationally accepted norms. In cases where the Model Law does not appear to have gained universal approval, we have been more cautious in adopting its terms. Where work is continuing at an international level on issues on which there is not currently consensus, but which may lead ultimately to consensus, we think it right to await those developments before recommending legislation for New Zealand. Ultimately, the business people of the world will determine the direction which they wish to take. The challenge for sovereign governments is to accommodate business needs by removing barriers to the extent to which they can, both properly and necessarily, consistent with the public policy of the sovereign State concerned.

7 In chapter 2,[36] we express our view that legal barriers to electronic commerce can be reduced to six generic categories: writing, signatures, originals, service of documents, physical presence or attendance, and negotiability. So far as is practicable *at the present*

---

[35] See chapter 2, The Need for Legislation, para 34.

[36] Paras 24–33.

*time*, we believe that our proposed Electronic Transactions Act will meet the needs of the business community in removing, or at least reducing the effect of, those barriers.

8 Generally speaking, we take the view that our proposed Electronic Transactions Act should operate to amend existing domestic laws which act as barriers to electronic commerce. This should be achieved in the same way that the requirement for "writing" has been overcome through the enactment of section 29 of the Interpretation Act 1999.[37] In effect, the Electronic Transactions Act will be applicable to all such transactions and its terms will have precedence over other statutes.

9 The discussion in ECom 1 was guided by four principles: choice, adaptation, technological neutrality, and compatibility,[38] as well as a commitment to the functional equivalent approach advocated by the Model Law.[39] The four guiding principles and the functional equivalent approach received widespread support from those who made submissions. Substantial support was also voiced in favour of the not dissimilar recommendations made by the Australian Electronic Commerce Expert Group's *Electronic Commerce: Building the Legal Framework* in which the Expert Group recommended (amongst other things):[40]

- removal of legal impediments to the implementation of electronic commerce; and
- ensuring certainty as to the application of the law to electronic commerce and enhancing business and consumer trust and confidence.

10 General support for a further principle emerged from the submissions: private sector leadership. The tenor of the suggested principle is that the online market should be driven by the private sector, with legislation only being warranted when it produces a more efficient outcome than self-regulation. In essence, a "wait,

---

[37] This comes into force on 1 November 1999. See also chapter 2, The Need for Legislation, para 28 and the Commission's report *A New Interpretation Act: To Avoid "Prolixity and Tautology": NZLC R17* (Wellington, 1990) on which the new Act is based. See, in particular, para 408 of that report.

[38] See ECom 1, paras 30–45 for a discussion of what the principles mean.

[39] The principles are set out in full in the executive summary in this report: see para E2.

[40] Electronic Commerce Expert Group *Electronic Commerce: Building the Legal Framework* (Australia, 1998) 4. The report can be found at http://www.law.gov.au/aghome/advisory/eceg.

see, assess and intervene only when necessary" approach. This principle is consistent with the emphasis on party autonomy in the Model Law.[41] We agree with it and adopt it for use in our work.

## NEW ZEALAND POLICY WORK

11 Mindful of the need for Government to inform business of its approach to electronic commerce, the Ministry of Commerce published *Electronic Commerce: The Freezer Ship of the 21st Century*. The purpose of that statement was to ". . . provide a framework for ongoing initiatives by bringing existing policy together and outlining the Government's overall policy approach".[42] That policy approach is

> one of minimal intervention and encouragement of self-regulation, consistent with the Government's overall policy framework. Government intervention will only be considered if it is necessary to address clearly identified market failures, or in order to maintain certainty for business and protection for consumers. Any intervention should consist of simple, predictable regulation that is technology-neutral . . . and able to respond to the pace of change in the electronic environment.[43]

This approach, in effect, endorses the principle of private sector leadership and the Law Commission's four guiding principles.

12 In order to coordinate work being done in the public sector, Cabinet directed the Ministry of Commerce, in conjunction with other government agencies, to develop a work programme on electronic commerce issues aimed at "maximising potential benefits and minimising potential pitfalls".[44] Coordination between departments was essential to avoid duplicity of effort. Responsibility for information industries crosses a number of government departments. However a number of interdepartmental interest groups were evident. As a result, five areas of public interest were identified:

---

[41] See article 4 of the Model Law, paras E3, 10, 53, 62, 333 of this report and paras 44–45 of the Guide to Enactment (appendix B).

[42] Ministry of Commerce, *Electronic Commerce: The Freezer Ship of the 21st Century* (Wellington, 1998) 8.

[43] Above n 42.

[44] Office of the Minister for Information Technology *Electronic Commerce; Report to Government Strategy Committee* (Wellington, 1998) para 2.1.

- Security Issues;
- Revenue Based Interests;
- Economic and Social Impacts;
- Consumer Protection, Privacy and Property; and
- Government Information Strategy.

Five Sector Committees were formed. Each Sector Committee has responsibility for one of the areas listed above. Representatives from each Committee make up the Electronic Commerce Steering Committee. The Steering Committee reports directly to the Minister for Information Technology and its brief is to assist Government in formulating policy on electronic commerce issues.[45] Appendix A sets out the structure and membership of these Committees.

## THE WIDER PICTURE

13 Recent reports issued by this Commission have noted some wider issues arising out of electronically generated communications.[46] The sorts of issues which need further consideration include:

- the use of electronic technology to enable citizens to gain access to legal services and to government agencies generally. This was alluded to in the Commission's report *Justice: The Experiences of Maori Women: Te Tikanga o te Ture: Te Mātauranga o ngā Wāhine Māori e pa ana ki tēnei* [47] and in the study paper prepared by (former) Commissioner Joanne Morris, *Women's Access to Legal Services: Women's Access to Justice He Putanga Mō Ngā Wāhine ki te Tika*; [48]
- the filing of electronic documents in court. Two members of the Commission have had the opportunity to visit the Bankruptcy Court of the Southern District of New York which operates in a paperless environment. It is apparent that significant cost savings for court resources are possible through

---

[45] The Information Technology Policy Group of the Ministry of Commerce has established a website (www.ecommerce.govt.nz) which provides links to information on government activities aimed to assist the development of electronic commerce.

[46] *Dishonestly Procuring Valuable Benefits: NZLC R51* (Wellington, 1998) and *Computer Misuse: NZLC R54* (Wellington, 1999).

[47] *NZLC R53* (Wellington, 1999) paras 147–151.

[48] *NZLC SP1* (Wellington, 1999) paras 103, 810 and 869.

providing services in this way. The extent to which these savings can be achieved in New Zealand is something on which further study is required; it is sufficient to say, for present purposes, that many of the current provisions of the High Court Rules 1985 and the District Court Rules 1992 create barriers to the use of electronically generated material,[49] and that we may be able to learn from the New York experience. We refer also to developments in New South Wales[50] and the UK;[51] and

- the need to synthesise (on an international basis) both the civil and the criminal law affecting the use of computers generally. There have been questions raised around the world in relation to the adequacy of existing criminal law to deal with computer misuse issues.[52]

There is a need to take an holistic approach to technologies which operate without respect for sovereign boundaries. The Model Law is a starting point for the civil law. In a paper presented to an APEC/WTC meeting in September this year,[53] the President of the Law Commission stressed the need for a global, systematic, and co-ordinated approach to criminal law issues in the electronic environment. The President noted that the borderless nature of

---

49 See chapter 2, para 31.

50 See the Practice Note issued on 15 March 1999 by Rt Hon Spigelman CJ entitled *Use of Technology in Civil Litigation* (May 1999) 45 (2) NSWLR v–xi.

51 In "How to court the IT revolution" *The Times*, London, United Kingdom, 31 August 1999, 21, Richard Susskind discusses the reforms for electronic case management proposed in Lord Woolf's Access to Justice paper, for which Susskind was the IT adviser. In addition the Scottish Court Service has established a website at www.scotcourts.gov.uk containing listings of judges and court opinions which can be searched. The purpose of the website is to ". . . benefit the administration of justice [and] improve public access to the law" (Gailey and Sibbald, "Scottish Courts Online" Computers and Law 3 10(2) (June/ July 1999) 6).

52 The chairman of the Senate's special committee on the Year 2000 problem, Senator Robert Bennett, has recently suggested that rather than disbanding after the year 2000 problem has passed, the panel may shift its focus towards an examination of the risks that business and government computers face from electronic attacks and subterfuge by terrorists and hostile foreign powers "Y2K Panel Won't Quit at 2000" *International Herald Tribune* 15 September 1999 3.

53 Hon Justice Baragwanath "Changes in International and Domestic Law which are Critical to a Borderless World of Electronic Commerce: An Update" (paper presented to APEC/WTC Conference, Auckland, 6 September 1999) available at the Law Commission's website www.lawcom.govt.nz.

computer crimes, and their potential to cause vast economic loss and physical damage, cry out for international measures to be taken against them. In his paper the President set out a number of ways in which computer crimes could be attacked; including a model criminal law akin to the Model UNCITRAL civil law, multilateral treaties and recognition of computer hacking as a crime at international law. The criminal law issues will be considered further over the next year by this Commission. Some introductory comments on the issues are made later in this report.[54]

## INTERNATIONAL DEVELOPMENTS

14 New Zealand has encouraged development of global solutions to electronic commerce issues through its membership of APEC, OECD and the World Trade Organisation. At the APEC Leaders meeting in Vancouver (November 1997) APEC Leaders agreed:

> that electronic commerce is one of the most important technological breakthroughs of this decade.

An APEC Electronic Task Force was established to manage APEC's work programme on electronic commerce, as set out in the *APEC Blueprint for Action of Electronic Commerce*.[55] The blueprint provides:

> The role of Government is to promote and facilitate the development and uptake of electronic commerce by
>
> - Providing a favourable environment, including the legal and regulatory aspects, which is predictable, transparent and consistent.
> - Providing an environment which promotes trust and confidence among electronic commerce participants . . .
> - Working with UNCITRAL and other international fora in moving forward work on legal foundations, where appropriate, for a seamless system of cross-border electronic commerce . . .

15 The leaders of APEC economies directed Ministers to establish a programme on electronic commerce for their region that will recognise the leading role of the business sector and promote a predictable and consistent legal and regulatory environment to reap the benefits of electronic commerce.

---

[54] See chapter 12, Criminal Law.

[55] Endorsed by the Ministers in Kuala Lumpur in 1998.

The New Zealand Government has taken up the challenge. These issues were explored further at a meeting of the Electronic Commerce Steering Group of APEC held in Auckland in June 1999.[56]

16 Similarly, the OECD is developing policies to deal with electronic commerce at a global level, particularly in the areas of consumer protection[57] and taxation.[58] The object is to provide a set of principles by which members of the OECD can regulate conduct within their territorial boundaries.

17 At UNCITRAL, the *Working Group on Electronic Commerce* is endeavoring to finalise uniform rules to deal more specifically with issues of "signature" in the electronic environment. A report is expected to be put before the full Commission meeting of UNCITRAL in mid 2000. These issues are discussed later in this report.[59]

18 The *Hague Conference on Private International Law* is in the process of developing a more sophisticated framework to deal with conflict of laws issues. As part of its work the Hague Conference held, in conjunction with the University of Geneva, a seminar from 2–4 September 1999 on private international law issues raised by electronic commerce. As a result of his contributions to the Hague Conference session in June 1999, Mr David Goddard, New Zealand's representative at that session, was invited to act as a co-rapporteur at the Geneva seminar. That appointment was recognition of New Zealand's role in raising electronic commerce issues at the June 1999 Hague Conference session. The work of the Hague Conference is discussed later in this report.[60]

19 The current Secretary of UNCITRAL, Dr Gerold Herrmann, has visited New Zealand on two occasions this year. His ideas on the way in which international trade laws can be harmonised are worthy of the greatest respect. He has identified obstacles to harmonisation and unification of international trade law as:

---

[56] For a report on the Steering Group's meeting see Brown "APEC on ecommerce" LawTalk 524, 2 August 1999, 11–12.

[57] See chapter 6, Consumer Issues, para 105.

[58] See chapter 18, Taxation, para 331.

[59] See chapter 9, Electronic Signatures, paras 152, 154–155, and appendix E which summarises overseas legislation in relation to electronic signatures.

[60] See chapter 14, Conflict of Laws, paras 279–282.

- different ideas of justice;
- different legal concepts and techniques;
- the "known devil" is preferred to the "unknown angel";
- rejection of novel law as synthetic compromise on lowest common denominator without supporting case law; and
- aversion by special-interest groups fearing disadvantages.[61]

20 As Dr Herrmann has suggested, these obstacles must be addressed by using the combined experience of experts from diverse regions and legal systems, with a view to preparation of a uniform text which can be expressed in plain terms in the six United Nations' languages: Arabic, Chinese, English, French, Russian and Spanish.[62]

21 In 1992 Shapira, a senior lecturer in law, identified a need for New Zealand to be involved in helping to shape the form of Model Laws and conventions which emerge from UNCITRAL's work.[63] In our view, the observations made by Shapira are even more relevant today. The development of the internet, and the ability to enter into international agreements through it, mean that now more than ever it is necessary for countries such as New Zealand to be represented at bodies such as UNCITRAL. As we may have little choice but to adopt many internationally developed Model Laws or Conventions, it makes sense that we are represented when both the agenda and content of such "laws" are being shaped.

---

[61] Summary (No 21) of address by Dr Herrmann to UNCITRAL "Congress on Uniform Commercial Law in the 21st Century", as discussed in G Shapira "UNCITRAL and its Work – Harmonisation and Unification of International Trade Law" [1992] NZLJ 309.

[62] Above n 61, 314.

[63] Above n 61, 314.

# 2
# The need for legislation

22 In ECOM 1 we identified a number of barriers to electronic commerce and raised questions as to the ways in which they could be removed. As a result of receiving submissions we have been able to crystallise our views on the nature of the barriers and the way in which they can best be removed.

23 We are of the view that New Zealand should enact an Electronic Transactions Act to remove the immediate barriers to electronic commerce. The Act should be facilitative in nature. By removing immediate barriers it should encourage the development of electronic commerce. The purpose of this chapter is to identify the barriers; note the competing public policy issues involved and cross-reference our discussion of the barriers and potential solutions to:

- other parts of this report;
- the provisions of the Model Law and the Guide to Enactment; and
- the Australian Bill.

We discuss the competing public interest factors with respect to each barrier later in this report.

24 We are satisfied that legal barriers to electronic commerce can be reduced to six categories. They are:

- statutory requirements that certain documents be "*in writing*";[64]
- statutory requirements that the "writing" be "*signed*";[65]
- the need to retain for various purposes "*original*" documents;[66]
- statutory requirements in relation to *notices and the service of documents* (whether by post or in person);[67]

---

64 See chapter 5, Statutory Overlay, paras 79–102.

65 See chapter 9, Electronic Signatures, paras 139–155.

66 See chapter 7, Evidence, paras 115–121 and chapter 8, Record Retention, paras 122–138.

67 See chapter 5, Statutory Overlay, paras 79–102.

- statutory requirements for *physical presence or attendance* of a person when things are done;[68] and
- the *negotiability* of electronically generated documents.[69]

25 Other barriers have been identified both by people who made submissions on ECom 1 and in other discussions which we have had with persons affected by our proposals. But, additional impediments which have been identified are equally applicable in the physical world. Examples given to us include the requirements for labelling of goods in various States and different customs requirements. Unless there is a complete harmonisation of laws relating to those, and other associated topics, such barriers will always remain.

26 In determining whether, and if so, to what extent, legislation should be enacted to remove the barriers which we have identified it is important to balance public interest considerations such as:

- the need for a minimalist approach so that the law is adapted to the needs of electronic commerce. This is consistent with our adaptability principle[70] and with existing government policy.[71] In our view, if a barrier can be removed *adequately* by contractual means that solution should be preferred to legislative intervention;
- the need for adequate statutory requirements to address the prevention of fraud;[72] and
- the need to avoid unnecessary transaction costs including, for example, legal costs incurred to resolve a legal point when the law is not sufficiently predictable.

We address these issues later in the context of each barrier.[73]

27 Issues involving "writing" and "originals" are, in our view, readily resolved. Issues involving "signatures" are more complex in nature

---

[68] See chapter 5, Statutory Overlay, paras 79–102.

[69] See chapter 4, Transportation Documents, paras 63–78.

[70] See executive summary, para E2, for a full statement of this principle.

[71] *Electronic Commerce: The Freezer Ship of the 21st Century*, 8; see also the Australian approach to which we referred in ECom 1, para 22.

[72] For a discussion of this public policy factor in a different context see *Cross-Border Insolvency: Should New Zealand adopt the UNCITRAL Model Law on Cross-Border Insolvency?: NZLC R52* (Wellington 1999), 2–4 and 112; see also P Millett *Tracing the Proceeds of Fraud* (1991) 107 LQR 71.

[73] See n 65–69 above for appropriate references.

and may require differing levels of solutions. Questions of personal presence or attendance will need to be addressed on an individual basis.[74] Negotiability is something which, in general terms, can be resolved by contractual rather than statutory means.[75]

28 So far as "writing" is concerned, electronically generated messages will, from 1 November 1999, qualify as "writing" as a result of the enactment of the Interpretation Act 1999 section 29. Section 29 plainly encompasses electronically generated information[76] by defining "writing" as:

> includ[ing] 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.

29 The requirement for "original" documents in an evidential sense will be met by recommendations made by this Commission in its report *Evidence: Reform of the Law*.[77] There remains a need to address the statutory requirements for "originals" in the context of record retention; our views on that issue are set out in chapter 8.[78]

30 We are recommending that the question of electronic signatures be dealt with, as an interim measure, by the adoption of legislation akin to article 7 of the Model Law. Inevitably, because of the way in which article 7 of the Model Law is expressed, questions of fact and degree will arise as to whether an electronic signature is sufficiently reliable to fulfil a requirement of law for a signature. In cases where there is no need for a witness to a signature or for a seal to be affixed, the level of reliability required could well be established to the satisfaction of a court by reference to the level of security attaching to the "signature" in a technological sense. In cases where the law requires an "enhanced" manual signature (by, for example, the addition of a witnesses' signature or the affixing of a seal) it is unlikely, in the meantime, that a court would

---

74 See chapter 5, Statutory Overlay, paras 79–102.

75 See chapter 4, Transportation Documents, paras 63–78.

76 See also *A New Interpretation Act: To Avoid "Prolixity and Tautology": NZLC R17* (Wellington 1990) on which the Interpretation Act 1999 was based; in particular para 408.

77 *NZLC R55 vol 1*, chapter 20, Documentary evidence and evidence produced by machine, device or technical process: *Evidence: Evidence Code and Commentary: NZLC R55 vol 2*, ss 117–123 and c410–429.

78 See paras 122–138.

permit such a signature to be made electronically. These issues are dealt with in more detail in chapter 9.[79]

31 Statutory requirements for the giving of notices or for the service of documents also pose problems. Our views, on which we expand later in this report,[80] are:

- If there is a statutory requirement to serve a document *personally* that statutory requirement should remain until such time as the legislature determines that the requirement is too onerous. Such provisions are enacted to ensure that particular documents are drawn to the attention of the persons upon whom they are served. Consequently, those requirements should remain in force until the need for such emphasis is demonstrated. An example is the need to serve court proceedings on a defendant personally. The initial service must be in person, although once an address for service is given by a solicitor acting for the litigant that address for service can include a postal address or a document exchange (DX) address or facsimile address, but not an email address.[81]
- If there is a statutory requirement that something be sent by ordinary post then, in our view, email should be regarded as the functional equivalent of ordinary post and service by email should be permitted *provided* the intended recipient has consented to receipt of the information by email through use of an application which can be read by the intended recipient. We refer, in this regard, to problems caused (for example) by the inability of one computer using "Word" to read information sent on "Word Perfect". Unless this requirement for consent is imposed, persons doing business electronically could, in effect, send messages in a language which the recipient cannot read: the functional equivalent of sending disclosure documents under the Credit Contracts Act 1981 by ordinary mail but written in Greek.[82]
- We believe that any safeguards imposed by statutes as to the time at which delivery by post will be effected should remain; an example is section 20 of the Credit Contracts Act 1981,

---

79 See paras 139–154.

80 see chapter 5, Statutory Overlay, paras 79–102.

81 See rr 44 and 206A High Court Rules 1985 and rr 43 and 233 District Courts Rules 1992. If a solicitor has not given notice that service can be effected by post or facsimile the solicitor cannot be compelled to receive service by those means: see *Invercargill City Council v Hamlin* (1994) 7 PRNZ 674 (CA).

82 See further, chapter 5, Statutory Overlay, paras 79–102.

which refers to delivery of disclosure documents under a credit contract. Section 20(2) makes it clear that the documents will not be deemed to be received until four days after they were posted. Other examples can be found in rule 206A of the High Court Rules 1985 and rule 233 of the District Court Rules 1992 as to the time when service by post or document exchange is deemed to be effected. Similar provisions should apply equally to email to preserve the principle of functional equivalence.

- If legislation requires service by *registered post*, then it is clear that the legislature has required a higher level of security to apply to such service than proof that the message was received in the ordinary course of the post. A functional equivalent of sending a document by registered post may be electronic delivery in circumstances where a reliable electronic acknowledgement of receipt can be produced by the person offering the document in evidence.
- If there is a statutory requirement that notice be given, but no particular form is prescribed, then it should be legal to give notice by email as long as there has been prior consent to the use of an application which can be read by the intended recipient.

We address some proposals for statutory reform in chapter 5.[83]

32 The next statutory requirement which creates barriers is the requirement for "presence" or "attendance" by people at a physical place where something is required to be done. An immediate problem is caused by the provisions of the Auctioneers Act 1928. The definition of the terms "sales by auction" and "sell by auction" suggest difficulty in carrying out a legal on-line auction.[84] Attendance is also an issue with regard to people who are required to witness documents: examples are affidavits filed for court proceedings.[85]

33 The final barrier which we have identified is one of negotiability. Documents such as Bills of Lading and Bills of Exchange are

---

[83] See paras 79–102.

[84] See Auctioneers Act 1928, s 2; see also chapter 5, Statutory Overlay, paras 79–102.

[85] See rr 27 and 510 High Court Rules 1985 and rr 25 and 508 District Courts Rules 1992. Note also the requirement for an original signature in r 27 High Court Rules 1985 and r 25 District Court Rules 1992 respectively although the court can grant leave to file an affidavit in facsimile form: *Hawkins v Young Hunter* (1997) 10 PRNZ 453; 455.

(usually) negotiable documents. The document is handed over as a document of title. The problems caused by "negotiability" are largely capable of solution by contractual rather than statutory models. We do not think a present need for legislation has been demonstrated. We refer to the discussions on negotiability contained in chapter 4 (Transportation Documents) which explains our reasons for not recommending changes to the law to meet perceived barriers caused by an inability to negotiate electronically generated instruments.[86]

34 We propose that the Electronic Transactions Act be confined to electronic transactions conducted "in trade". The term "trade" is broadly defined by the Fair Trading Act 1986 to mean:

> any trade, business, industry, profession, occupation, activity of commerce, or undertaking relating to the supply or acquisition of goods or services or to the disposition or acquisition of any interest in land.[87]

By limiting the application of the Electronic Transactions Act to electronic transactions conducted "in trade" we avoid the need to list individually many of the legal requirements we wish to exempt from the Act's application such as wills and affidavits and the method of delivery of government services. In the case of the delivery of government services, it is especially important that the responsible government agency is given the opportunity to consider whether its services can be delivered electronically and, if so, in what technological application. Once that has been done, the government agency can then recommend any necessary legislative changes to accommodate delivery of its services in electronic form.

35 We now discuss the issues raised in this chapter in more detail by reference to particular aspects of the law.

---

[86] See paras 66–73, 77–78.

[87] Fair Trading Act 1986, s 2.

# 3
# Contract

## ELEMENTS OF CONTRACT

36 UNDER NEW ZEALAND LAW, to prove that a binding contact has been formed:

- the parties must have *intended to create legal relations* at the time of entry into the agreement;[88]
- an *offer* must have been made and that offer *accepted* by another party;[89]
- *valuable consideration* must back the promises contained in the agreement;[90] and
- the terms of contract must be *certain*.[91]

These legal criteria apply to determine whether there is a binding contract regardless of whether the contract is formed orally, by paper-based writing, through conduct or through electronic means. There is also the overarching requirement that persons entering into a contract have the legal capacity to do so.[92] While this requirement is not influenced by the medium in which a contract is concluded, the anonymous nature of the internet increases the opportunity for contracts to be concluded with persons who do not have the legal capacity to contract; in this regard we note that the Minors' Contracts Act 1969 may be in need of review.[93]

---

88 ECom 1, paras 55–64.

89 ECom 1, paras 65–74.

90 ECom 1, paras 75–77.

91 ECom 1, paras 78–81.

92 See generally, JF Burrows, J Finn and S Todd *Law of Contract in New Zealand* (8th ed), 1997 chapter 13.

93 Contracts formed with minors, depending upon the circumstances (ie age of the minor, marital status, nature of the contract), may be unenforceable. See Burrows, Finn and Todd (8th ed), 1997 441–450. See also *Morrow & Benjamin Ltd v Whittington* [1989] 3 NZLR 122 and Lip, "Minor's Civil Law Capacity to Contract on the Internet" submission to the Queensland Law Reform Commission available at www.jcu.edu.au. "Minor" is not defined by the Minors' Contracts Act 1969; full age is reached for all the purposes of the law of New Zealand at 20 years: Age of Majority Act 1970, s 4(1).

## Intention to create legal relations and certainty of terms

37 None of the submissions made to us in response to ECom 1 suggested that there was any need to reform the law in relation to the elements of intention to create legal relations and certainty of terms. There is nothing we can usefully add to our discussion of these topics in ECom 1.

## Offer and acceptance

38 In ECom 1 we described the law on offer and acceptance.[94] When dealing with websites it is important to establish at the outset whether a "proposal" (to use a neutral word) found on a website is, as a matter of law, an invitation to treat or an offer. An invitation to treat, as opposed to an offer, cannot be turned into a binding contract by mere acceptance of its terms. A business offering goods or services over the internet will generally want to retain control over the quantity of goods or services it sells, and must therefore ensure that its website contains invitations to treat. If the website advertisement of a product or service is considered an offer, website sellers ". . . may find they have entered into an unserviceable number of contracts."[95]

39 Another influential factor in the formation of contracts is the time when acceptance is deemed to have occurred. A contract is complete upon acceptance, which is the time the acceptance is received by the offeror, unless the postal acceptance rule applies. (The postal acceptance rule and case law interpretation of that rule were discussed in ECom 1.)[96] If the means of communication of acceptance is one that would *not* be categorised by the court as instantaneous,[97] then the timing of dispatch of an electronically generated message is, instead of the time of receipt, the time when an acceptance is deemed to have been received by the offeror, and also the time when the contract is complete. The law is uncertain

---

94 ECom 1, paras 65–67 (offer) and 68–74 (acceptance).

95 G Crowhen and S Grace "The Legal Implications of Doing Business Electronically: Business Application of the Law of Contract to E-Commerce", paper presented to Institute for International Research conference February 1999, 9.

96 ECom 1, paras 69 and 70. To those cases we would add the case of *Henthorn v Fraser* [1892] 2 ch 27.

97 See the discussion of when the postal acceptance rule applies in ECom 1, paras 70–74.

in this area because it is difficult to predict whether the postal acceptance rule will apply to an acceptance sent electronically.[98]

40 We posed the question, in ECom 1, whether acceptance of an offer through electronic means should only be completed upon proof that it *actually* reached the offeror.[99] A number of submitters supported the statutory abolition of the postal acceptance rule for all modes of communication, including by electronic means. In our view, there are strong reasons to abolish the postal acceptance rule in New Zealand. Quite apart from its debatable application in the electronic environment,[100] it is undesirable to have different rules as to when acceptance of an offer occurs depending upon whether the contract is domestic or international in nature.[101] But, on reflection, we have misgivings about making a final recommendation to abolish the postal acceptance rule when submissions were sought by us on this issue in the context of a report dealing solely with electronic commerce. It is conceivable that many of those who choose to do business solely through paper-based means through the postal system may wish the rule to remain in force. Moreover, the prospect of abolishing the postal acceptance rule was not so starkly stated in ECom 1.[102]

41 There are a number of issues which have arisen from consideration of the application of that law of contract to the electronic

---

98 In ECom 1, although we did not expressly state that the "law is uncertain" we did so by implication when we said: "The first question is whether it is appropriate to classify acceptance of an offer using electronic communications as one which falls within the general ambit of an instantaneous communication . . . If the communication was made by email the answer depends on whether the email user had direct and immediate access to the person to whom the email is sent or whether the email was sent through the electronic equivalent of the postal service, an internet service provider (ISP), which collected the mail. Users in the former category have a mode of communication which is close to instantaneous while those using an ISP may only communicate as quickly as their telephone access, service provider and personal inclination dictate": para 71 and subsequently, when discussing article 15 of the Model Law, article 15 "eliminates the confusion caused by the possible application of the postal acceptance rule by deeming messages to be received when they enter the addressee's designated information system: para 90.

99 ECom 1, para 74.

100 We use the word "debatable" because the postal acceptance rule may only apply to certain types of electronically generated messages depending upon whether the message is classified as instantaneous or not: see the discussion of this issue in ECom 1, paras 69–74.

101 For an explanation of the different rules that apply to international contracts for the sale of goods see ECom 1, paras 72–74.

102 ECom 1, para 74.

environment which are beyond the scope of a report confined to electronic commerce. Accordingly, we will issue a separate discussion paper dealing, among other things,[103] with the possible abolition of the postal acceptance rule.

42 We deal later in this chapter with the question whether default rules for attribution of electronically generated messages, timing of electronically generated messages and acknowledgement of receipt of electronically generated messages should be enacted in a form consistent with articles 13, 14 and 15 of the Model Law.[104]

### Consideration

43 In ECom 1 we raised the question whether the doctrine of consideration should continue to be an essential element of binding contracts,[105] while noting that it was beyond the scope of ECom 1 to consider whether consideration should continue to be an element of contract. Not surprisingly, in the context in which the question was raised, there was no support for abolition of the doctrine of consideration as part of legislation designed to facilitate electronic commerce. The merits of abolition of the element of consideration is something which the Law Commission may give its attention to at some future time.

## STATUTORY OVERLAY

44 In ECom 1 we dealt specifically with barriers to the formation of contracts arising from overarching statutory provisions.[106] We referred to the formalities required to execute a deed,[107] to assign debts and choses in action,[108] for contracts relating to land and guarantees;[109] and more generally, to other statutory instruments which deal with international sales of goods, shipping and carriage by air.[110]

---

[103] See ECom 1, para 48 and n 118.

[104] ECom 1, paras 49–61.

[105] ECom 1, Q31 and paras 75–77.

[106] ECom 1, paras 100–111.

[107] Property Law Act 1952, s 4; ECom 1, paras 100–105.

[108] Property Law Act 1952, s 130; ECom 1, paras 106–107.

[109] Contracts Enforcement Act 1956, s 2; ECom 1, paras 109–111.

[110] ECom 1, paras 112–136; in particular we address the Sale of Goods (United Nations Convention) Act 1994, the Maritime Transport Act 1994, the Marine Insurance Act 1908 and the Carriage by Air Act 1967.

45 In contrast to ECom 1, in this report we discuss barriers resulting from statutory overlay and the use of transportation documentation separately from our discussion of the law of contracts.[111] We have already outlined the precise barriers caused by statute,[112] and it is those barriers to which we direct further attention later in this report.[113]

### *The Contracts Enforcement Act*

46 One of the statutory barriers to the formation of contracts by electronic means not discussed separately in this report is the requirement for writing and signature imposed by the Contracts Enforcement Act 1956 section 2(2). Section 2(2) provides:

> No contract to which this section applies shall be enforceable by action unless the contract or some memorandum or note thereof is in writing and is signed by the party to be charged therewith or by some other person lawfully authorised by him.

That section applies to contracts relating to land and guarantees.[114] Section 29 of the Interpretation Act 1999 will (from 1 November 1999) enable electronic communications to constitute "writing". Whether or not an electronic equivalent to a manual signature will be sufficient to comply with the requirements for a signature under section 2(2) of the Contracts Enforcement Act will ultimately turn upon whether a court assesses the reliability of the electronic signature to be sufficiently reliable for the purpose for which it is used, having regard to the nature of the transaction.[115] In most cases, a simple email message, with a person's name typed at the foot, would, in our view, be insufficient to constitute a "signature" for contracts relating to land and guarantees. However, a court might find the signature sufficient if, for instance, the amount involved is of low value or the transaction is not complex or the parties have completed contracts by electronic means

---

[111] See chapter 5, Statutory Overlay and chapter 4, Transportation Documents.

[112] See para 24 above; the barriers identified are writing, signature, original, service of documents, physical presence or attendance and negotiability.

[113] See chapters 4, Transportation Documents; 5, Statutory Overlay; 7, Evidence; 8, Record Retention; and 9, Electronic Signatures.

[114] Contracts Enforcement Act 1956, s 2(1).

[115] See chapter 9, Electronic Signatures and particularly para 149 and, for a discussion of the Interpretation Act 1999, para 5, 28 and 80–81.

previously.[116] Equally, there is a potential for an electronic signature which meets a high level of security to be accepted as sufficient for Contract Enforcement Act 1956 purposes. But, ultimately, each case will need to be determined on its own facts.

47 The Commission, in its discussion paper *Repeal of the Contracts Enforcement Act* (PP 30), concluded:

> The Commission considers that candour requires it to state clearly its present view that the time has now come for the repeal without replacement of all of the Contracts Enforcement Act 1956. We emphasise, however, that this present view is not fixed or rigid, and that we are open to persuasion that it is mistaken.[117]

Although we have not yet been dissuaded from that conclusion, it is inappropriate for us to recommend repeal of the Contracts Enforcement Act 1956 in a report confined to electronic commerce. Accordingly, we propose to detail submissions received in response to PP30, examine the merits of repealing the Contracts Enforcement Act and make final recommendations for reform in a later report.[118]

## QUESTIONS OF ATTRIBUTION

48 In ECom 1 we asked the question whether there should be statutory rules which attribute liability for electronic messages.[119] Article 13 of the Model Law deals with questions of attribution (and was discussed in ECom 1).[120] Article 13(2) deems an electronically generated message to be that of the originator if it was sent by a person who has the authority to act on behalf of the originator in respect of that message or if it was sent by an information system programmed by, or on behalf of, the originator to operate automatically.

49 The Australian (Federal) Attorney-General's Electronic Commerce Expert Group, in its report of 31 March 1998 to the

---

[116] The law of estoppel and the law of part performance may also prevent a party from avoiding a contract for land or guarantees entered into by electronic means. See *NZLC PP30*, paras 7–9.

[117] *NZLC PP30*, para 41; See also DF Dugdale "Formal Requirements: the Proposed Repeal of the New Zealand Contracts Enforcement Act 1956" (1998) 13 Journal of Contract Law 268.

[118] See paras 40–41.

[119] ECom 1, Summary of Questions, Q5 and xvi.

[120] ECom 1, paras 94–99.

Attorney-General, took the view that it was preferable to *not* enact article 13(2) of the Model Law, instead leaving development of this area to the common law.[121] That recommendation is reflected in the Australian Bill.[122]

50 If article 13 had the effect of codifying the rules of common law and equity relating to both agency and estoppel there would be benefit in adopting it. The law of estoppel, even now, may be regarded as in a state of development. Codification of the law of agency and estoppel *could* enhance predictability of outcome and, by doing so, reduce transactions costs by making the legal outcome in a particular case clearer, and thereby reducing recourse to litigation. However, article 13 does not go far enough to achieve predictability of outcome.

51 Those parts of article 13 which, on their face, seem to be a codification of the relevant law of estoppel and agency are merely indicators which can be taken into account in determining whether a message should or should not be attributed to a particular person. The Guide to Enactment of the Model Law stated that the purpose of article 13 was not to assign responsibility but, rather, to deal with attribution of data messages by establishing a presumption that under certain circumstances a data message would be considered as a message of the originator.[123] The provisions of article 13 are based on article 5 of the UNCITRAL Model Law on International Credit Transfers.[124] Paragraph 92 of the Guide to Enactment records that earlier drafts of article 13 had contained an additional paragraph expressing the principle that attribution of authorship of a data message to an originator should not interfere with the legal consequences of that message which should be determined by other applicable rules of national law. Although that principle is not set out in the Model Law, paragraph 92 of the Guide to Enactment makes it clear that the principle was considered sufficiently important to be restated in the Guide. Domestic laws of agency were not intended to be affected by article 13.[125]

52 The Australian approach makes it very clear that the question of attribution is to be determined by domestic law, whether written

---

[121] Electronic Commerce Expert Group Report *Electronic Commerce: Building the Legal Framework*, paras 4.5.63–4.5.79.

[122] Electronic Transactions Bill, cl 15(2).

[123] Guide to Enactment, para 83.

[124] Guide to Enactment, para 83.

[125] Guide to Enactment, para 84.

or unwritten.[126] On reflection, we prefer the Australian approach, at least in the short term. Other reasons cementing that view include:

- Applying the private sector leadership principle, encouragement should be given to participants in the market to develop contractual solutions tailored to their particular case in preference to rules which operate across-the-board to allocate risk to a particular party in all circumstances.
- The whole question of attribution is closely linked to the question of what can constitute an electronic version of a manual signature. For reasons set out at paras 149–154 of this report, we recommend some aspects of "signatures" be deferred until further international work is completed.[127] Once further international work has been completed, then New Zealand should liaise closely with Australia on future changes to the law so that, if practicable, there can be a harmonisation of rules in relation to attribution, which will restrict problems which would otherwise flow from conflicts of laws,[128] at least at a Trans-Tasman level.

## QUESTIONS OF TIMING AND ACKNOWLEDGEMENT OF RECEIPT

### *Timing*

53 So far as timing issues are concerned, they are, in our view, dealt with adequately by default provisions of the type contemplated by article 15 of the Model Law.[129] The default rules provided for by article 15 can be displaced by agreement to the contrary; hence, party autonomy is retained.[130] The time of receipt of an electronically generated message is, under article 15(2), intended to be

---

[126] Electronic Transactions Bill, cl 15(2).

[127] See chapter 9, Electronic Signatures.

[128] See in general chapter 14, Conflict of Laws. See also "NOIE deputy chief to head up new National Electronic Authentication Council" 6(13) Electronic Commerce Report 4.

[129] ECom 1, paras 90–93.

[130] The most recent *draft* of the Auckland District Law Society/Real Estate Institute of New Zealand agreement for sale and purchase of land contains a good example of how the default rule might be displaced by agreement to the contrary. In that draft (eg cl 1.2(3)(d)) provision has been made for receipt of email to be proved by reference to the time at which it is acknowledged by the party or by the solicitor orally or by return email or otherwise in writing. We note that the reference to "in writing" may require reevaluation having regard to the enactment of s 29 of the Interpretation Act 1999.

the time at which the message entered the designated information system of the recipient or, if it was sent to an information system which was not the designated information system, at the time when the message was retrieved.[131] But if no designated information system has been given by the addressee, the default rule provides that receipt occurs when it enters an information system of the addressee.[132]

54 We gave consideration to the possibility of limiting adoption of article 15 to those provisions of it that pertain to the time and place of *receipt* of electronic communications. We thought that may be appropriate because we were attracted to abolishing the postal acceptance rule; thus, questions of dispatch would no longer have been relevant. But, as we are not recommending abolition of the postal acceptance rule in this report,[133] it is essential to provide for both receipt and dispatch. Otherwise, the postal acceptance rule *may* apply, creating uncertainty as to the time of formation of a contract.[134] As was stated in ECom 1, article 15

> . . . eliminates the confusion caused by the possible application of the postal acceptance rule by deeming messages to be received when they enter the addressee's designated information system.[135]

55 Beyond removing uncertainty as to the application of the postal acceptance rule, article 15 has several other advantages which recommend its adoption. Article 15:

- provides for the circumstance where a party has more than one place of business and the sender of a message chooses the place of business which has the closest relationship to the underlying transaction.[136] Inclusion of such a provision avoids disputes about the effectiveness of delivery and, where the place of receipt is relevant to this, questions of jurisdiction and applicable law;[137]

---

[131] Model Law, article 15(2)(a).

[132] Model Law, article 15(2)(b).

[133] See paras 40–41.

[134] See para 39.

[135] ECom 1, para 91.

[136] Model Law, article 15(4)(a).

[137] See generally chapter 14, Conflict of Laws and ECom 1, chapter 6.

- creates a rule that is useful for localising a transaction which is delocalised in nature and, by determining the place of dispatch, may provide a would-be litigant with a jurisdictional tie to New Zealand;[138]
- in providing default rules, creates efficiencies for the majority of traffic that utilises the internet, that being "low value, high volume" transactions; and
- will in all likelihood be adopted by many of our trading partners, giving rise to consistency of approach at an international level. The Australian Bill adopts the substance of article 15 of the Model Law but has reorganised its content into the headings: time of dispatch; time of receipt; and place of dispatch and receipt.[139]

56 Factors militating against adoption of article 15 are:

- to create special rules as to timing for the electronic environment would be contrary to the technological neutrality principle;
- there are doubts as to whether the default rules contained in article 15 will solve a sufficient number of problems which cannot be cured by contractual provisions. In essence, this amounts to a fear that adoption of article 15 will provide a "solution" for which there is no demonstrated need;[140] and
- there is a question over whether it is appropriate for Government to dictate a set of rules which may or may not accord with industry practice. This offends against the private sector leadership principle.

---

[138] See rule 219 of the High Court Rules and rule 242 of the District Courts Rules.

[139] The Explanatory Memorandum to the Australian Bill (http://law.gov.au/ecommerce/interim3.html) when discussing cl 14 states: "Clause 14 is largely based upon Article 15 of the UNCITRAL Model Law". See also, s 15 of the Electronic Transactions Act 1998 (Singapore).

[140] R Hill "The Internet, Electronic Commerce and Dispute Resolution: Comments" Journal of International Arbitration, 103 he states: "Arsic notes that the question of the time at which contracts are formed by electronic data interchange (EDI) remains unsettled. This is true and the matter has been studied for years. However, despite its interest to legal theorists, the matter does not appear to be of much practical significance. Indeed, EDI contracts are usually governed by an EDI Trading Agreement, formed by conventional means, and the question of the time of formation has not given rise to any known disputes" (footnotes omitted).

57 The submissions received that commented on article 15 were divided on whether to adopt it. Three examples are:

> The enactment of a provision similar to Article 15 would create the certainty required to determine when information or a document has been sent and received, which is essential in setting the legal terms of electronic commerce.[141]
>
> Telecom does not consider there is any need to legislate in order to promote certainty in electronic transactions. Areas where there may be some initial doubt such as issues of timing will best be resolved by contract.[142]
>
> . . . New Zealand legislation should enact principles similar to those set out in article 15 of the Model Law in order to recognise the fact that not all electronic communications are instantaneous. Unlike telephone, facsimile and telex communications, transmissions via the Internet are typically not instantaneous. Messages sent by the Internet not infrequently require several minutes to arrive at their destination . . . The law relating to contract formation and time of acceptance needs to recognise this inherent delay.[143]

58 In our view the factors in favour of adopting article 15 outweigh those against. While we agree that article 15 can be seen as providing a set of rules which may discourage parties from entering into agreements tailored to their own needs, we think it is preferable, given the wide variety of participants utilising electronic commerce, that default rules should be in place which are more certain and which are tailored to the electronic environment, but out of which the parties can still contract. Larger players in the market may well devise their own rules, but the same cannot be said for the smaller to medium sized businesses or consumers who elect to trade on the internet.

### *Acknowledgement of receipt*

59 Article 14 of the Model Law deals with "acknowledgement of receipt". The Guide to Enactment states:

> The use of functional acknowledgements is a business decision to be made by users of electronic commerce; the Model Law does not intend to impose the use of any such procedure. However, taking into account

---

[141] Submission of the Ministry of Commerce and the Ministry of Consumer Affairs, 7, para 22.

[142] Submission of Telecom New Zealand Ltd, para 9.

[143] Submission of Information Technology Association of New Zealand 10.

> the commercial value of a system of acknowledgement of receipt and the widespread use of such systems in the context of electronic commerce, it was felt that the Model Law should address a number of legal issues arising from the use of acknowledgement procedures. It should be noted that the notion of "acknowledgement" is sometimes used to cover a variety of procedures, ranging from a mere acknowledgement of receipt of an unspecified message to an expression of agreement with the content of a specific data message. In many instances, the procedure of "acknowledgement" would parallel the system known as "return receipt requested" in postal systems.[144]

The Guide to Enactment goes on to say that:

> Article 14 is not intended to deal with the legal consequences that may flow from sending an acknowledgement of receipt, apart from establishing receipt of the data message.[145]

60 The Australian Electronic Commerce Expert Group recommended that legislation was not needed to deal with the issue of acknowledgements.[146] A provision equivalent to article 14 has not been included in the Australian Bill. We agree with the approach adopted by members of the Electronic Commerce Expert Group when they said:[147]

> We have taken the approach that legislation should only be considered to facilitate the implementation and conduct of electronic commerce in Australia and have therefore only recommended legislative intervention where necessary to avoid uncertainty or to remove obstacles to the use of electronic commerce. To the extent that existing legislation or common law deals with these issues, it is our view that the same situation should apply to electronic commerce; discrimination between media should be avoided.

We do not believe that article 14 enhances predictability of outcome as it would not obviate reliance on the common law. Contractual solutions are preferable.[148] Accordingly, we recommend that article 14 not be adopted.

---

144 Guide to Enactment, para 93.

145 Above n para 144.

146 Electronic Commerce Expert Group *Electronic Commerce: Building the Legal Framework* paras 4.5.80–4.5.83 and recommendation 13.

147 Above n 146, para 4.5.83.

148 Such as those contained in the seventh draft of the Auckland District Law Society/Real Estate Institute of New Zealand Agreement for Sale and Purchase, cl 1.2(3)(d) see n 130 above.

## MISCELLANEOUS PROVISIONS OF THE MODEL LAW

61 The relative novelty of electronic commerce can be a barrier to the development of trust.[149] "Trust" is a notion to which reference is often made in discussions of how to facilitate electronic commerce; but, it can also be an ill-defined concept. In our view, in this context, "trust" has two important parts, ie:

- confidence that what is being done electronically has the same legitimacy that it would have if done with paper; and
- an assurance that the user will not be disadvantaged by the use of the electronic medium.[150]

62 It is not possible for the legislature to instill users of electronic commerce with the necessary trust of the technology. We are of the firm view that this industry – more than any other because of its nature – should be private sector led. While the legislature cannot directly instill trust in users of electronic commerce, it is open for it to provide an Electronic Transactions Act that is comprehensive in approach, even if, from a legal perspective, some provisions are not strictly necessary to remove an existing barrier as to form. Such *legally* redundant provisions do however play a part in reassuring users of electronic commerce that their business practices are legitimate. In short, as was recommended by the Australian Electronic Commerce Expert Group in *Electronic Commerce: Building the Legal Framework* the approach taken in what is now the Australian Bill should ensure "certainty as to the application of the law to electronic commerce and enhance business and consumer trust and confidence".[151] To bolster business

---

[149] An example of this lack of trust is given by the Ministry of Commerce: ". . . consumers are willing to give their credit card numbers to complete strangers when completing a purchase by telephone, yet hesitate to send their credit card details over the Internet to a well established Web based vendor such as Amazon.Com.Secure": *Electronic Commerce: The Freezer Ship of the 21st Century* 18.

[150] An example of being "disadvantaged" would be an Internet Service Provider being exposed to greater liability than its real world counterpart.

[151] (Australia 1998) 4.

confidence and trust in the use of electronic commerce, we recommend adoption of articles 4 (Party Autonomy),[152] 5 (Non-Discrimination)[153] and 5 bis (Incorporation by Reference) of the Model Law.[154]

---

[152] See paras 44–45 of the Guide to Enactment.

[153] See para 46 of the Guide to Enactment.

[154] See paras 46.1–46.7 of the Guide to Enactment.

# 4
# Transportation documents

63 ARTICLES 16 AND 17 OF THE MODEL LAW deal with transportation documents. Their main purpose seems to be the promotion of confidence in the use of electronically generated information. The purpose of both articles 16 and 17 is to ensure that the actions to which references are made can be performed electronically without causing prejudice to those who choose to trade in that way.[155]

64 Some of the actions listed are not required by law to be performed "in writing" or "signed". Others, such as those given to holders of "received for shipment" bills of lading by the Mercantile Law Amendment Act 1922,[156] are based on signed documents.

65 A barrier to electronic commerce is negotiability of documents of title. As we pointed out in ECom 1,[157] the practical barrier to the introduction of an electronic equivalent of a bill of lading is the need for an infrastructure to enable the person, for the time being entitled to the bundle of rights flowing from the bill of lading, to verify the validity of a particular transaction so that he or she can be confident that what has been transferred does in fact represent title to goods which he or she has acquired.

## Negotiability

66 Articles 16 and 17 of the Model Law apply to all forms of carriage of goods. But, it is only in relation to the bill of lading that the question of negotiability arises. All other documents to which the articles refer will be capable of being given legal effect through

---

[155] See further, Guide to Enactment, paras 108–122.

[156] Mercantile Law Amendment Act 1922, s 3(1). "'Received for shipment' bills of lading" is defined to mean a shipping document issued in accordance with s 3(1), signed by a person purporting to be authorised to sign the same, and acknowledging that the goods to which the document relates have been received for Shipment: Mercantile Law Amendment Act 1922, s 3(1).

[157] ECom 1, para 125.

the change to the definition of the term "writing" brought about by the passage of section 29 of the Interpretation Act 1999.[158]

67 In the paper-based environment, a negotiable bill of lading is a unique document upon which shippers, consignees, endorsees and banks can rely to provide title to goods in transit by sea. In endeavoring to apply the same standard of "uniqueness" to an electronically generated document, article 17(3) of the Model Law (in its final form) has created a difficulty.[159] As Howland puts it:

> When considering the creating of a right and the transferring of it to one person, a view amongst the UNCITRAL delegates was that a method could be regarded as satisfactory, if it could be described as rendering a message or messages "unique". Supporting this, there was a view that the notion of "uniqueness" was not unknown to practitioners of transport law and users of transport documents. It was felt by some that, if the description "unique" is applied to the messages, it could perhaps be assumed that this would indicate sufficiently that there is at any one time only one right or obligation and only one recipient of it.
>
> However, when States are considering adopting this text into their bodies of law, some legislators may feel the need to give more attention to this language in order to avoid any possible misunderstandings, because some doubt has been expressed about the adequacy of this word "unique". Drafters of legislation will need to remember that *all* electronic messages are, in any case, *always* and *necessarily* unique – each with its own addressee, its own time of dispatch, its own contents. They will remember, too, that under some registry-based methods, a single initial allocation of a right or a single transfer of it to one person will use several separate individual messages, not just one; so the word "unique" must not be made to mean "only one" message. Furthermore,

---

[158] See para 28.

[159] This view should be compared with paras 115–117 of the Guide to Enactment which refer to a "guarantee of singularity". In para 117 the UNCITRAL Secretariat noted that the term "unique" may lend itself to misinterpretation but, having considered the risk of misinterpretation, noted that the Commission had decided to "retain the reference to the concepts of uniqueness of the data message and uniqueness of the transfer for the purposes of Article 17, in view of the fact that notions of 'uniqueness' or 'singularity' of transport documents were not unknown to practitioners of transport law and users of transport documents . . . It was decided, however, that this Guide should clarify that the words 'a reliable method is used to render such data message or messages unique' should be interpreted as referring to the use of a reliable method to secure that data messages purporting to convey any right or obligation of a person might not be used by, or on behalf of, that person inconsistently with any other data messages by which the right or obligation was conveyed by or on behalf of that person".

they will realise that several sets of messages could be sent to several different persons at the same time or in quick succession, purporting to transfer the same right. Each of the messages and, indeed, each of the transfers, would be in themselves "unique"; yet all but one of them may be fraudulent.[160]

68 The essence of the points made by Mr Howland is that it is important to ensure only one recipient (and no other person) obtains the benefit of the transfer of title to goods which is inherent in the notion of an electronic functional equivalent to a bill of lading.

69 It is also important to note that at the 32nd Session of UNCITRAL in 1999 there was discussion about further coordination and cooperation on the topic of transport law. In the report of the 32nd session UNCITRAL noted: [161]

> . . . it appeared that further harmonization in the field of transport law would greatly benefit international trade. The working group had found a number of issues that had not been covered by the current unifying instruments. Some of the issues were regulated by national laws which, however, were not internationally harmonized. Evaluated in the context of electronic commerce, that lack of harmonization became even more significant. It was also reported that the working group had identified numerous interfaces between the different types of contracts involved in international trade and transport of goods (such as sales contracts, contracts of carriage, insurance contracts, letters of credit, freight forwarding contracts, as well as a number of other ancillary contracts). The working group intended to clarify the nature and function of those interfaces and to collect and analyse the rules currently governing them. That exercise would at a later stage include a re-evaluation of principles of liability as to their capability with a broader area of rules on the carriage of goods.

Accordingly, further work in this area is likely.

## Negotiable instruments

70 We are of the view that the barrier of "negotiability" is essentially a market based problem rather than a legal problem. It is to be noted that there are no *express* requirements in either the Hague-Visby Rules or the Mercantile Law Act 1908 for bills of lading to be produced in paper form or to be signed in order to be valid as an

---

[160] R Howland "UNCITRAL Model Law on Electronic Commerce" (1997) 32(6) European Transport Law 703, 707. Mr Howland was one of the United Kingdom delegates to UNCITRAL at the time of approval of the Model Law.

[161] A/54/17, 53–54, para 412.

instrument transferring title to goods.[162] Now that the term "writing" has been defined, as a matter of New Zealand law, to include electronically generated information[163] the legal obstacles created by form requirements have been removed.

71 It is important that we explain further our view that the problem of "negotiability" is essentially a market based problem rather than a legal problem. In ECom 1 we mentioned the Bolero project.[164] The Bolero system is a contractual system which provides a rule book by which all participants are bound which supplies the infrastructure required to ensure that title can be passed to goods in transit from vendor to purchaser through the means of a functional equivalent of a bill of lading. The infrastructure is important as there needs to be a register of interests in some form (whether electronic or otherwise) which provides a method by which those who are using electronic means to transfer title in this way can check whether the person from whom they are buying is shown as the person entitled to transfer goods. Such a "register" must either be established by the State under some regulatory means or through contractual means – such as the Bolero system. There is no enthusiasm in New Zealand for the notion that the Government should, by legislation, create a register which can be used for this purpose although, in principle, there is very little difference between this type of register and the type of register used under the Motor Vehicle Securities Act 1989 or under the proposed Personal Property Securities Act.[165]

72 Our concern as to the adequacy of article 17 of the Model Law is more directed to the absence of an infrastructure through which it can operate than anything else; although we are also persuaded that there is merit in the argument raised by Howland that there are difficulties with the notion of "uniqueness" in the context of electronically generated messages.[166]

73 The Hague-Visby Rules do not apply to non-negotiable instruments. The non-negotiable instrument, not being a document of title, faces no obstacles to being replaced by electronic waybills.

---

[162] ECom 1, para 121. See also para 77 of this report.

[163] Interpretation Act 1999, s 29.

[164] ECom 1, paras 124–125.

[165] This lack of enthusiasm for a statutory register was evident in responses made to Q6 of ECom 1; see also ECom 1, 47, where the question was posed whether special legislation was necessary to facilitate the use of electronic bills of lading.

[166] See paras 67–68.

## CONTRACTS FOR SHIPMENT OF GOODS BY AIR

74 Contracts for the shipment of goods by air are governed by the Carriage by Air Act 1967. Section 7 of that Act gives force to the Warsaw Convention and to the Guadalajara Convention. The principal document provided for by the Warsaw Convention associated with contracts for carriage of goods is the air waybill. Although the Warsaw Convention provides that air waybills may be either negotiable or non-negotiable, in practice air waybills are used as non-negotiable instruments. As was stated in ECom 1 (para 129),

> . . . given the speed of air transport there would seem to be little reason to issue a negotiable air waybill. (para 129)

Hence air waybills function as *prima facie* receipts and evidence of the contract of carriage: article 11(1).

75 We noted that the "Warsaw Convention as it applies in New Zealand does not appear to permit air waybills to be issued electronically" because of provisions that contemplated a physical delivery of the air waybill.[167] To remove these impediments to the use of electronic air waybills we recommended adoption of the Montreal Protocol No 4, and set out the relevant article at para 132. [168]

76 Since the Commission's release of ECom 1, the Civil Aviation Amendment Act 1999 has been passed and comes into force 1 December 1999.[169] As reported by the Transport and Environment Committee (at Select Committee stage), passing the Civil Aviation Amendment Bill will implement Montreal Protocol No 4 and, in doing so,

> . . . enable[s] the use of electronic waybills, which would result in compliance cost saving in terms of reduced paperwork and allow for the more expeditious processing of consignments.[170]

---

[167] Signature requirements are not an issue as the signature of a carrier may be stamped and that of the consignor may be printed or stamped: G Crowhen and S Grace "The Legal Implications of Doing Business Electronically: Business Application of the Law of Contract to E-Commerce" (Institute for International Research Conference, Wellington, 24–25 February 1999) 22, para 4.8.30.

[168] Our reference to the Montreal Protocol No 3 in ECom 1, paras 132–133 was in error. In para 132 of ECom 1 what is set out is actually Montreal Protocol no 4.

[169] Civil Aviation Amendment Act 1999 Commencement Order 1999 (SR 1999/280).

[170] Report of the Transport and Environment Committee (no 245–2) ii.

## SHOULD NEW ZEALAND ADOPT ARTICLES 16 AND 17 OF THE MODEL LAW?

77 We are not persuaded at present that articles 16 and 17 should be enacted as part of the law of New Zealand at present. We take that view for the following reasons:

- Save for negotiable bills of lading, the definition of the term "writing" contained in section 29 of the Interpretation Act 1999 will solve any potential for discrimination of electronically generated documents.
- There are no requirements of law involving "signature" which would prevent title to goods in transit from passing from vendor to purchaser simply because any contract for the sale of those goods had been entered into in electronic form.
- The Hague and the Hague-Visby Rules, which have force of law in New Zealand through section 209 of the Maritime Transport Act 1994 and the Mercantile Law Amendment Act 1994, do not expressly require bills of lading to be issued in paper but, we accept, that the references to "possession", "delivery" and "endorsement" in sections 13A–13C of the Mercantile Law Act 1908 (as amended by the Mercantile Law Amendment Act 1994) may be interpreted as requiring the existence of a physical document. It is noted that when an amendment was made to section 13 of the 1908 Act in 1994, that the issue of the medium was not directly addressed.[171] The Hamburg Rules, to which we referred in ECom 1,[172] anticipate electronic bills of lading but those rules have not been adopted under New Zealand law. While the Mercantile Law Amendment Act 1994 contains a provision permitting regulations to be passed to cover the use of electronic equivalents to a bill of lading, no such regulations have yet been passed.[173]
- Questions of negotiability can be resolved by contractual means.[174] Pending much greater international adoption of the Hamburg Rules, we believe that the market should be encouraged to find contractual solutions. Only if contractual solutions prove to be insufficient should legislation be considered.

---

[171] ECom 1, para 121 and P Myburgh "Bits, Bytes and Bills of Lading: EDI and New Zealand Maritime Law" [1993] NZLJ 324.

[172] ECom 1, para 126.

[173] Mercantile Law Act 1908, s 13(5).

[174] See para 72.

New Zealand should await results of further international work, in particular the work identified by UNCITRAL by its 32nd session in 1999,[175] before deciding whether to enact provisions akin to articles 16 and 17 of the Model Law. Certainly no practical problems have been raised with us to suggest there is a need for immediate legislative action. In our view New Zealand should await further developments at an international level before making a final determination on whether legislation is necessary.

78 Further submissions on these issues are sought.

---

[175] See para 69.

# 5
# Statutory overlay

79 AS DISCUSSED IN CHAPTER 2, major barriers to electronic commerce derive from statutory requirements as to form.[176] In this chapter we deal with statutory requirements as to –

- writing
- service of documents (whether by post or in person)
- physical presence or attendance of persons when things are done.

Barriers caused through the need for writing to be *signed*, for certain documents to be retained or produced in *original* form and difficulties with the *negotiability* of electronically generated documents are discussed later in this report.[177]

## WRITING

80 The statutory requirement for writing has been overcome by the enactment of section 29 of the Interpretation Act 1999 (previously section 28 of the Interpretation Bill 1997), which follows a recommendation to that effect made by this Commission in 1990.[178] The 1999 Act came into force on 1 November 1999. Section 29 defines "writing" as:

> includ[ing] 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.

Thus a statutory requirement for "writing" will now be met by communication through electronic means. Where the statute provides that the "writing" must be *signed* there is an additional

---

[176] Above para 24.

[177] See chapter 9, Electronic Signatures, paras 153–155, chapter 7, Evidence, paras 117–121, chapter 8, Record Retention, paras 123–137, and chapter 4, Transportation Documents, paras 65–73 respectively.

[178] *A New Interpretation Act: To Avoid "Prolixity and Tautology": NZLC R 17*; see in particular, para 408.

impediment to overcome. By way of example, an assignment of copyright carried out electronically will not be effective unless the court can also be satisfied that it has been "signed" in accordance with section 114 of the Copyright Act 1994; likewise, a guarantee or an agreement for the sale and purchase of land will not be enforceable unless the requirement of a "signature" is met under section 2 of the Contracts Enforcement Act 1956. The issue of signature is discussed further in chapter 9.[179]

81 The enactment of the Interpretation Act 1999 removes the *need* for definition of the word "writing" in the Electronic Transactions Act. However, for completeness, we recommend that the term be included in an Electronic Transactions Act and given the meaning attributed to it by section 29 of the Interpretation Act 1999.[180]

## SERVICE OF DOCUMENTS

### *Background*

82 A number of statutory provisions require documents to be posted or hand delivered. A distinction is sometimes drawn between ordinary and registered post; some statutes require service by ordinary post,[181] while others require service by registered post.[182]

83 We do not propose to refer to all statutes which require particular forms of service; instead we will simply give examples of statutes. The principles which we identify will be applicable to all statutes which deal with those particular modes of delivery. We do not differentiate between the giving of notices and the service of documents for the purpose of this analysis.

### *Delivery by ordinary post*

84 By way of example, section 20 of the Credit Contracts Act 1981 provides:

---

[179] See chapter 9, Electronic Signatures, paras 153–155.

[180] It is hoped that the inclusion of the term will increase public confidence in the legal status of electronic communications. See above paras 61–62.

[181] For example s 20 Credit Contracts Act 1981.

[182] "Registered post" is defined in the Immigration Act 1987 s 2 as including "any service that provides a system of recorded delivery and is similar in nature to the registered post service provided by New Zealand Post". Other statutes which require notice to be given by registered post include the Tax Administration Act 1994 ss 136–137 and the Unit Titles Act 1972 s 38.

**20. Method of disclosure—**

(1) Subject to subsections (2) and (3) of this section, initial disclosure, [guarantee disclosure,] modification disclosure, continuing disclosure, and request disclosure shall each be made by giving, or sending by post to the last place of residence or business known to the creditor or to an address specified by the person for this purpose, to each person to whom disclosure is to be made, disclosure documents that comply with section 21 of this Act:
Provided that where that place of residence or business or address is the same for 2 or more [debtors], disclosure documents given or sent to any of those [debtors] shall be deemed to have been given or sent to all those [debtors].

(2) For the purposes of sections 22 [, 24, and 24A,] when disclosure is made by sending disclosure documents to a person by post, the disclosure shall be deemed to be made to the person on the 4th working day after the day on which the documents are posted.

(3) For the purposes of sections 25 to 28 of this Act, when disclosure is made by sending disclosure documents to a person by post, the disclosure shall be deemed to be made to the person on the day on which the documents are posted.

(4) Where disclosure that is required to be made to more than one person is made to those persons on different days, it shall for the purposes of this Act be deemed to be made to all those persons on the last such day.

85 Section 20(2) deems service (for specific purposes) to be effected within a certain period from the day on which the documents are put into the post. The reason for such requirement is easy to see. There is an assumption that the document will reach the intended recipient in the ordinary course of the post. However it is unknown at what point the recipient will retrieve the document from his or her mailbox and read it. The legislature has no control over when a document may be read, but can make certain assumptions as to a reasonable time within which the document will be delivered. The assumption made is reflected in section 20(2) of the Credit Contracts Act 1981.

86 The same considerations apply equally to retrieval of mail sent electronically. In some cases, a person may not have access to his or her computer for a number of days. The person may choose not to open his or her mail or to make contact with the Internet Service Provider to gain access to the mail box. If email is to be regarded as the functional equivalent of ordinary mail then, in our view, the same safeguards for intended recipients which apply to delivery by post should apply equally to delivery by email. In terms of section 20(2) of the Credit Contracts Act 1981, for example, disclosure of documents sent electronically would be deemed to be made on the fourth working day after the day on which the email was sent.

87 There is, however, one important difference. If documents are sent by email they may be sent through the use of an application which cannot be read by the intended recipient. Obviously, if the intended recipient communicates first by electronic means, it can readily be inferred that communication through the same means is acceptable. But receipt of an email from a person does not necessarily mean that a reply, which includes an attachment which is generated through a different application, can be read.

88 To accommodate this peculiarity, it should be necessary, consistent with the choice principle, for a person who wishes to give notice or to serve documents by email, in lieu of ordinary post, to be able to establish to the satisfaction of the court both

- that the intended recipient actually agreed to receipt of the notice by email; and
- that the particular form of email used can be read by the intended recipient.

In our view there should be no prescriptive legislation detailing how such agreement should be proved; that should be a matter left to the parties to determine. If documents are sent in lieu of statutory notice and these factors cannot be proved by the person who sent the documents then the service will be invalid. That is a risk which the person seeking to use email runs. The onus will be on the person who wishes to serve or give notice by email to prove agreement on the points raised.

89 There will usually be sanctions available against a person who has failed to comply with obligations as to service. For example, a lender who has not made disclosure under the Credit Contracts Act 1981 may, in the absence of relief being granted by the court under section 31 or section 32 of that Act, be prevented from recovering amounts otherwise extinguished by the Act.[183] Another example is the failure to serve court proceedings in the prescribed manner. A judgment entered in consequence of a proceeding which has been served irregularly may be set aside as a matter of right.[184] The question is whether there are any circumstances which ought properly to distinguish service by ordinary post from service by email. We think that there are. For example, while most people may, as a matter of course, go on holiday and make arrangements

---

[183] *The Laws of New Zealand: Consumer Credit and Hire Purchase* (Butterworths, Wellington, 1992) vol 7, paras 41–49.

[184] High Court Rules r 5; District Court Rules r 5.

for mail to be collected, they may not make similar arrangements with regard to email. If service was permitted by email, in lieu of ordinary post, then there may need to be education about the consequences, particularly for consumers. For those reasons we believe proof of actual consent to receipt of notices or service by email should be required.[185]

### *Delivery by registered post*

90 Other statutes[186] require service of documents by registered post. The use of registered post indicates that the legislature requires a higher degree of security as to service than reliance on an assumption that documents are delivered in the ordinary course of the post. As mentioned previously,[187] a functional equivalent of the sending of a document by registered post would be the electronic delivery in circumstances where an electronic acknowledgement of receipt can be produced by the person offering the document in evidence.

91 In our view, if legislation sets the higher standard of service by registered post, an electronic equivalent is not appropriate, at least in the meantime. The position is similar to that which pertains to electronic signatures. Given that we are not recommending adoption of the UNCITRAL Model Law provision dealing with acknowledgements of receipt,[188] it would be inappropriate to legislate for electronic receipt of information required to be delivered, by law, through registered post.

92 Questions of functional equivalence for service by ordinary post or by registered post (or, indeed, by way of delivery to a document exchange) are not dealt with in the Model Law and were not raised in ECom 1. We do not have adequate information about the likely consequences of allowing service by email (in the absence of express consent as to mode or form) as a functional equivalent of service by ordinary post. We note, however, that in its recent publication *Bright Future: 5 Steps Ahead: Making ideas work for New Zealand* the Government said that it was –

> . . . determined to reduce the volume and complexity of the law through a general tidy-up. Over time many laws have become redundant or out of date. Government departments that administer

---

185 See para 88.

186 Above n 182.

187 Above para 86.

188 Above para 60.

> laws will be required to conduct a cull of regulations. This will aim to remove unnecessary statutes and amalgamate laws where possible. Government wants to achieve a 12–25% reduction in the number of regulations over the next 12 months.[189]

In our view a review of all statutes and subordinate legislation in which service by ordinary post and registered post is required should be conducted as part of that review, so that decisions can be made on whether to permit service by email as a functional equivalent. In the meantime we would recommend, as an interim measure, that service by email could be effected where service by ordinary post would be sufficient if there is express consent personally signed in a paper form which consents both to receipt of notices by email and confirms ability to receive electronic transmissions through the application which will be used to send them. This provision would enable those who wish to do all business by email to do so without fear of unintentional, yet adverse, legal consequences.[190]

### *Personal service*

93 Where a statute requires documents to be delivered personally an even higher standard of security is required in relation to proof of receipt. Service of court proceedings is an obvious example. In our view such requirements should remain and, at least at this stage, not be given any electronic equivalent as a matter of law. It should be open, however, for parties to designate an electronic means of receiving documents (whether by facsimile or email) once steps have been taken in relation to court proceedings.[191]

---

[189] Ministry of Commerce (1999) 52.

[190] We refer in particular to a submission dated 20 August 1999 from ASB Bank Limited which referred to the disclosure requirements of the Credit Contracts Act 1981 causing difficulties to the bank through inability to meet *customer* demand for presentation of such material in an electronic form. While we can see good reason to ensure that the use of electronic media is not foisted upon those who do not wish to use it for this purpose, we can see no reason to prevent service by email where it is clear that there is customer consent and, indeed, demand for it. We note that in the United States the Federal Reserve Board has issued an interim ruling that allows banks to send customers electronic statements with prior approval. The relevant press release (dated 31 August 1999) can be read at http://www.bog.frb.fed.us/boarddocs/press/BoardActs/1999/19990901/. Furthermore we note that those provisions of the Securities Act 1978 which require documents to be sent to investors do permit communication by "electronic or other means that enables the recipient to readily store the matter in a permanent and legible form" (s 2).

[191] This would necessitate an amendment to both the High Court Rules 1985 and the District Court Rules: compare n 85.

## PHYSICAL PRESENCE OR ATTENDANCE

94 Certain statutes require things to be done in the presence of a human being. They can also require things to be done at a physical location. An example of the former requirement is the need for affidavits to be witnessed by persons who see the deponent swear that the content of the document is true and correct.[192] An example of the latter requirement is statutory provisions requiring certain information to be displayed at registered offices. For instance, licensed auctioneers and motor vehicle dealers must display prominently at their place of business and all branch offices a notice with the name and licence details of the auctioneer or dealer.[193]

95 The Government has recently moved to facilitate the ability of licensed motor vehicle dealers to sell cars directly over the internet. Initially, section 54(1) of the Motor Vehicle Dealers Act 1975 provided that no licensed dealer may carry on business at any place other than the place of business named on the licence (or a branch or subsidiary office) but, by section 8(1) of the Motor Vehicle Dealers Amendment Act 1999, which came into force on 13 September 1999, the Act was amended to allow a licensee to conduct its business at any place while continuing to require the licensee to have at least one place of business at which appropriate notices could be posted.[194] The amendment was prompted by a dispute between Korean carmaker Daewoo and the Motor Vehicle Dealers Institute regarding the "Daewoo Direct" programme for selling cars via an 0800 toll-free number.[195]

96 By way of contrast, the Auctioneers Act 1928 has changed little since its enactment.[196] Nobody in 1928 could have contemplated

---

[192] See above n 85.

[193] Auctioneers Act 1928 s 30; Motor Vehicle Dealers Act 1975 s 55.

[194] Motor Vehicles Dealers Act 1975 s 54(2) as amended by the Motor Vehicle Dealers Amendment Act 1999 s 8(1) and SR 1999/260/2. "New motor vehicle business" is defined in section 2 as "such part of the business of a motor vehicle dealer as consists of the business of purchasing, selling, exchanging, or leasing of new motor vehicles (whether as principal or agent); and includes the purchase or acceptance of a trade-in in connection with the purchase of a new motor vehicle".

[195] See "Web no site for Arthur Daley" *The New Zealand Herald*, 5 May 1999.

[196] It has been described as having "a style of control and supervision that is now unfashionable" and has arguably outlived its usefulness (*The Laws of New Zealand: Auction*, vol 1, para 1).

the modern situation whereby "auctions" take place online[197] with the auctioneer and bidders located not only in different rooms or buildings, but often in different countries. Online auctions can take various forms, but one example is where an airline posts a minimum bidding price for a ticket on its website, and a person seeking to purchase it specifies or "bids" the price he or she would be willing to pay for that ticket. The airline then tries to meet this price in order to sell an otherwise empty seat; the higher the bid, the more likelihood of a seat.[198] Unlike an auction in the physical world, where the "reserve" selling price is not usually known unless it is reached, the bidder knows the minimum price the airline will accept for the ticket before the auction starts.

97 While the Auctioneers Act 1928 does not actually require that the auctioneer and bidders be physically present during an auction in so many words, this requirement seems implicit from the section 2 definition of "sales by auction".[199] The critical part of the definition is the use of the word "outcry" which is, itself, defined by section 2 of the Act as including

> any request, inducement, puff, device, or incitement made or used by means of signs, speech, or otherwise in the presence of not less than 6 people by any person for the purpose of selling any property . . . .

98 Whether online auctions fall within the regulatory scheme provided in the Auctioneers Act 1928 depends on whether the

---

[197] The term "online" has been defined as "enjoying a network connection to another computer". See C Gringas *The Laws of the Internet* (Butterworths, London, 1997) 385.

[198] See R Abeyratne "Auctions on the Internet of Airline Tickets" (1999) 4(1) Communications Law 22.

[199] The full definition reads: "Sales by auction" or "sell by auction" means the selling of property of any kind, or any interest or supposed interest in any property, *by outcry*, by the auctioneer saying "I'll take" and commencing at a higher figure and going to a lower figure, by what is known as Dutch auction, knocking-down of hammer, candle, lot, parcel, instrument, machine, or any other mode whereby the highest, the lowest, or any bidder is the purchaser, or whereby the first person who claims the property submitted for sale at a certain price named by the person acting as auctioneer is the purchaser, or where there is a competition for the purchase of any property or any interest therein in any way commonly known and understood to be by way of auction; and shall be deemed to include the selling of any property by outcry in any public place, as the same is defined in the [Summary Offences Act 1981], or in any room, or mart, or place to which the public are admitted or have access, whether or not the sale of the goods has been advertised to take place. (emphasis added)

acceptance of an online bid is considered to be "made or used by means of signs, speech or otherwise in the presence of not less than six people . . ." in accordance with the definition of "outcry" in section 2. Under a literal interpretation, the acceptance of an online bid could be considered to be made "by outcry" if six other people were huddled around the auctioneer's computer at the relevant time. However it does seem possible that a court would consider that sales where the auctioneer and bidders are in separate locations could never have been intended to be covered by the Auctioneers Act 1928.

99 When construing the definition in section 2 a court is likely to take into account the policy reasons for requiring the presence of six other people, and consider whether these reasons could be satisfied within the electronic environment. Possible reasons for the requirement could be to ensure a fair auction process, or to provide a certain level of competition in the bidding. A court is likely to consider whether these requirements could be met in an online bidding situation when determining if the definition of "outcry" is met.

100 While there have been very few cases that deal with the relevant provisions of the Auctioneers Act 1928, in *National Australia Finance Ltd v Tolra*[200] Master Williams QC (as he then was) seemed to accept that it would be legally impossible under the Act to hold an auction with less than six people present.

101 It is undesirable that statutes which were designed to meet particular needs in earlier times should operate in a manner which may discourage electronic commerce. In each case it will be necessary to identify the particular policy issues which required the restrictions at the time the legislation was enacted and then to determine whether those policy considerations can be met in the electronic environment. An additional question is, of course, whether the policy reasons are still justified. It seems to us that it is entirely undesirable for a person conducting an auction online to be unsure whether he or she is conducting a valid auction. We recommend that urgent attention be given to this particular matter by the Ministry of Commerce which, we understand, has already embarked upon some work in this area. The speed with which the Government reacted to the problems caused by the way in which the Motor Vehicle Dealers Act 1975 was framed, indicates that it is appropriate to reconsider these issues promptly.

---

[200] Unreported (26 January 1993) High Court Wellington, CP735/92, 5 and 10.

102 We have already recommended that various government agencies responsible for the administration of legislation should carry out a review of all legislation under their control to see whether that legislation is likely to discourage electronic commerce. Given that the underlying rationale for requiring physical presence or attendance will vary markedly from statute to statute, we believe it is neither appropriate nor desirable to seek to amend existing laws through the enactment of a generic statute dealing with electronic transactions. We remain happy to assist other ministries or agencies in reviewing this area of law.

---

# 6
# Consumer issues

103 It is clear from a footnote to article 1 that the Model Law ought not override any rule of law intended for the protection of consumers. However, that exclusion from the Model Law results more from the terms of reference under which UNCITRAL operates than from any reasoned or concluded view that exemption of consumer protections is justified. UNCITRAL was created in 1966 as an organ of the Sixth Committee of the General Assembly of the United Nations.[201] That resolution authorised UNCITRAL to prepare or promote the adoption of conventions, Model Laws and uniform laws. In those days, international trade law regulated international trade in an almost exclusively business to business sense. It is only with subsequent developments such the ease of international travel by aircraft and the development of the internet which has brought consumer transactions within this general sphere.

104 The potential implications for consumers in the increasing use of electronic commerce were recognised by the Ministry of Consumer Affairs in its 1997 discussion paper, *Electronic Commerce and the New Zealand Consumer: Issues and Strategies for the Future*, which raised the issues for public debate.

105 In ECom 1 we examined electronic commerce from the perspective of those involved in international trade on a business to business basis.[202] This was done to focus issues of law reform on the potential benefits which could be gained from international trade, given that New Zealand earns its living from export earnings. It was noted that the OECD was addressing matters relating to protecting the interests of consumers who were engaged in commerce on the internet, and that recommendations were due to be concluded in

[201] Resolution 2205 (XXI) of 17 December 1966.

[202] ECom 1, para 3.

October 1998.[203] The work of the OECD on this issue is not yet concluded, but is scheduled to be completed by the end of 1999. The Ministry of Consumer Affairs is representing New Zealand at that forum.

106 In the Guide to Enactment of the Model Law[204] it is expressly stated that the Model Law had been drafted without special attention being given to issues which might arise in the context of consumer protection. The Guide to Enactment then states –

> At the same time, it was felt that there was no reason why situations involving consumers should be excluded from the scope of the Model Law by way of a general provision, particularly since the provisions of the Model Law might be found appropriate for consumer protection, depending on legislation in each enacting State. Footnote ** [to Article 1] thus recognises that any such consumer protection law may take precedence over the provisions in the Model Law. Legislators may wish to consider whether the piece of legislation enacting the Model Law should apply to consumers. The question of which individuals or corporate bodies would be regarded as "consumers" is left to applicable law outside the Model Law.[205]

## ELECTRONIC TRANSACTIONS FRAMEWORK

107 The thrust of this report is to recommend adoption of an Electronic Transactions Act for New Zealand which is similar to that currently before the Federal Parliament in Australia but more limited in its scope.[206] The issue which we now address is whether there are any reasons, stemming from the need for consumer protection, which militate against the Act applying generally to both business to business, and business to consumer transactions.

108 In general, we believe it is appropriate for any Electronic Transactions Act passed by the New Zealand Parliament to apply equally to business to business and consumer to business transactions. The Ministry of Consumer Affairs has drawn to our attention that in the United States of America, the National

---

[203] In ECom 1, para 3 we referred to the OECD's Draft Recommendation Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce which was due to be concluded in October 1998. The Guidelines cover issues of concern to consumers including privacy (see further chapter 11 Privacy), and the application of consumer protection across borders (see further chapter 14 Conflict of Laws).

[204] Guide to Enactment, para 27.

[205] Guide to Enactment, para 27.

[206] See appendix C and the comments in para 5 regarding limiting proposed legislation to electronic transactions conducted "in trade".

Conference of Commissioners on Uniform State Laws established a task force to consider this issue in the context of the proposed (American) Uniform Electronic Transactions Act.[207] The task force decided that consumer transactions should not be exempted with the reason for that decision resting primarily on the expected growth of electronic consumer transactions.

109 The Ministry of Consumer Affairs has advised us[208] that it has reservations about protections for consumers arising out of statutory provisions requiring delivery or service of notices or other documents and the retention of copies. Otherwise, the Ministry generally agrees with the views reached by the United States task force.

110 On the question of delivery or service of notices or other forms of documents, we have already referred to problems which arise out of the media specific way in which legislation is currently drafted.[209] We have recommended no change in the meantime to the law but, rather, a review of particular statutes to see whether service of documents by email is appropriate.[210] That recommendation should meet the concern validly expressed by the Ministry of Consumer Affairs in relation to the delivery of notices. Our further recommendation would enable service to be effected by email where consent was given in writing, on a paper based document, prior to the need for delivery or service to be effected which recorded the intended recipient's consent to receipt of information by email using a particular type of application.[211] In our view, those recommendations adequately meet the concerns of the Ministry of Consumer Affairs.

111 We have made recommendations concerning retention of records later in this report which we believe meet adequately the concerns expressed by the Ministry of Consumer Affairs.[212] In addition, the liability of customers for unauthorised electronic banking transactions was also mentioned by the Ministry, and this issue is also discussed later in this report.[213]

---

[207] Letter from Ministry of Consumer Affairs to Law Commission dated 9 August 1999.

[208] Above n 207.

[209] Chapter 5, Statutory Overlay, paras 82–93.

[210] Above para 92.

[211] Above para 92.

[212] See chapter 8, Record Retention, paras 133–135.

[213] See chapter 15, Banking, paras 294–312.

112 In coming to the view that any Electronic Transactions Act should apply equally to consumer transactions, we also bear in mind that:

- in a New Zealand context it is difficult to apply the term "rule of law intended for the protection of consumers"[214] in any practical sense. Many statutes which contain consumer protection provisions apply across the whole range of business activity. The Credit Contracts Act 1981 and the Fair Trading Act 1986 are notable examples;[215]
- the OECD Guidelines on Consumer Protection in the Context of Electronic Commerce also strive towards functional equivalency and technological neutrality as general principles, while recommending safeguards for consumer protection;
- it would be difficult, if not impossible, to articulate a generic description of the type of consumer transaction which would be excluded from the operations of an Electronic Transactions Act.

113 The policy considerations for specific safeguards in relation to legislative requirements for writing and signing are identified in Sneddon, *Legislating to Facilitate Electronic Signatures and Records: Exceptions, Standards and the Impact of the Statute Book*.[216] These considerations are evidentiary (ensuring availability of admissible and reliable evidence), cautionary/protective (encouraging deliberation and reflection before signing), record keeping (creating a durable record which facilitates regulation), and channelling (clarifying whether the parties intend to act in a legally significant way). In relation to consumer contracts being formed online we suggest that:

- It is necessary to differentiate provisions dealing with contracts from those relating to advertising. The question is whether the appropriate demarcation is available in an electronic environment.
- There is a need for pre-contractual and contractual information to be accessible to the consumer.
- Consumers should have the ability to keep copies of the agreements for future reference.
- Substantive requirements as to the format and font size may be necessary.

---

[214] Model Law, article 1, n **.

[215] Generally, *The Laws of New Zealand: Consumer Protection* (Butterworths, Wellington, 1992) vol 7, para 1.

[216] (1998) 21(2) UNSWLJ 334, 347–348.

- Subsequent communications, such as statements of account and notices of variation should only be sent electronically when the consumer has expressly consented to this.[217] There may be a need for appropriate rules to limit a supplier's liability where it is fair and reasonable (possibly relating to attribution and the like) in a manner akin to section 68A(3) of the Trade Practices Act 1974 (Australia).[218]

114 The Ministry of Consumer Affairs is currently undertaking a review of consumer credit law and policy and intends to report to Cabinet with recommendations for legislative reform by mid 2001. Electronic commerce issues which arise in the context of consumer credit will be covered as part of that review, and the Ministry intends to release a consultation document discussing these issues in May 2000. Submissions on the matters raised in this chapter should be made directly to the Ministry of Consumer Affairs.

---

[217] We dealt with this issue in chapter 5, Statutory Overlay, para 92.

[218] Section 68A(3) provides:

> (3) In determining for the purposes of subsection (2) whether or not reliance on a term of a contract is fair or reasonable, a court shall have regard to all the circumstances of the case and in particular to the following matters:
>
> (a) the strength of the bargaining positions of the corporation and the person to whom the goods or services were supplied (in this subsection referred to as "the buyer") relative to each other, taking into account, among other things, the availability of equivalent goods or services and suitable alternative sources of supply;
>
> (b) whether the buyer received an inducement to agree to the term or, in agreeing to the term, had an opportunity of acquiring the goods or services or equivalent goods or services from any source of supply under a contract that did not include that term;
>
> (c) whether the buyer knew or ought reasonably to have known of the existence and extent of the term (having regard, among other things, to any custom of the trade and any previous course of dealing between the parties); and
>
> (d) in the case of the supply of goods, whether the goods were manufactured, processed or adapted to the special order of the buyer.

# 7
# Evidence

## THE EVIDENCE REFERENCE

115 In 1989 the then minister of justice referred the reform of the law of evidence to the Law Commission. The main object of the reform project was:

> To make the law of evidence as clear, simple and accessible as practicable, and to facilitate the fair, just and speedy judicial resolution of disputes.[219]

116 It was necessary to review the law of evidence systematically. The Commission published a number of discussion papers on various discrete aspects of the law of evidence. One of those discussion papers concerned documentary evidence and judicial notice.[220] As a touchstone for dealing with evidential issues in the context of an electronic environment we cited with approval, in ECom 1,[221] an observation made by Butler-Sloss LJ in *Re M & R (Minors)*[222] where her Ladyship said –

> The law of evidence should not be subtle and difficult to understand. And fine distinctions should only be tolerated if both unavoidable and . . . easy to make.

117 We expressed the view in ECom 1 that the proposed Evidence Code (which would be the final product of the evidence reference) would provide sufficient clarity to evidence law as it applies to electronic commerce. We said that:

> The draft Evidence Code will enable those engaged in electronic commerce to carry on business without avoidable uncertainty as to whether electronically-generated information can be admitted as evidence in court. The Commission is also of the view that the changes

---

219 *Evidence NZLC R55* vol 1, para 6.

220 *Evidence Law: Documentary Evidence and Judicial Notice: NZLC PP22* (Wellington, 1994).

221 ECom 1, paras 193–200 generally.

222 [1996] 4 All ER 239 (CA) 254.

it will propose to the law relating to documentary evidence will meet concerns of professionals such as auditors.[223]

118 The Evidence Code recommended by the Law Commission deals, in Part 6, with documentary evidence and evidence produced by machines, devices or technical processes. We refer to sections 117–123 (inclusive) of the Evidence Code which, [224] for convenience, are reproduced as appendix D to this report. The commentary contained in paras C406–C429 (inclusive) of the Evidence Code summarises the effect of these provisions.

119 Two submissions had been made to us questioning whether the proposed definition of the term "document" in the Evidence Code did meet the needs of electronic commerce. We set out below excerpts from the Commission's report *Evidence – Reform of the Law* containing our comments on those submissions.[225]

> 513 In *Electronic Commerce Part 1: A Guide for the Legal and Business Community* (NZLC R50, 1998) the Commission considered the recommendations proposed for documentary evidence in the final Evidence Report would ". . . meet the needs of electronic commerce by facilitating the production of electronically generated evidence" (para 193). In response to the Electronic Commerce Report, two submissions questioned the proposed definition of "document" in the Code because the definition appeared to include not only the information stored in a computer, but the computer itself.
>
> 514 The Code defines "document" as a "record of information". Thus, a computer would be a document only if, for example, its service contains writing that is relevant evidence in a proceeding. Ordinarily the "document" would be that part of the computer that contains the relevant electronic data, i.e. a particular portion of the hard disk. The problems identified by the commentators to the Electronic Commerce Report relate not so much to the definition of "document" as to the process of discovery. The concern is that the existence of relevant information stored on a computer would make the computer itself discoverable. That, however, is not an evidentiary issue, but one of procedure which has to be left to the exercise of common sense by counsel and the judiciary. (For further clarification on the distinction between "discovering" information contained on a computer and "discovering" information contained on paper see paras 217 and 218 of the [first] Electronic Commerce Report).

---

[223] ECom 1, para 238.

[224] *Evidence NZLC R55* vol 2.

[225] *Evidence NZLC R55* vol 1, paras 513 and 514.

## THE MODEL LAW PROVISIONS

120 Articles 8 and 9 of the Model Law deal, respectively, with the need for "original" information and the admissibility and evidential weight of electronically generated messages. In our view, the provisions of the Evidence Code meet the *evidential* problems which articles 8 and 9 of the Model Law seek to cure.[226] Article 8, however, continues to have relevance to the need for information to be "retained" by other provisions in the law. We deal with that retention aspect of article 8 separately.[227]

121 We recommend that the Evidence Code, which allows for electronic material to be used as evidence in legal proceedings, be enacted at the same time as our proposed Electronic Transactions Act. In this way, all immediate barriers to electronic commerce can be addressed contemporaneously in appropriate legislation.

---

[226] See paras 62–71 (inclusive) of the Guide to Enactment. For ease of reference we set out in appendix B to this report the Model Law with the Guide to Enactment produced by the Secretariat of UNCITRAL. In appendix D we have reproduced those provisions of the Evidence Code recommended by this Commission in its August 1999 report.

[227] See chapter 8, Record Retention, para 136.

# 8
# Record retention

122 In ECOM 1 submissions were sought as to whether New Zealand should adopt article 10 of the Model Law. Article 10(1) provides that: "Where the law requires that certain documents, records or information be retained that requirement is met by retaining data messages . . .". Article 10 is facilitative. It does not *require* records to be kept in electronic form; it *allows* them to be retained in that form if persons choose to do so. An advantage of enacting an equivalent to article 10 is that it would apply across the board, avoiding the need to amend every piece of legislation pertaining to record keeping. This approach reflects the reality that many businesses and government departments keep records, in electronic form, and that recent legislation allows this to be done. [228]

123 Article 8, which deals with "original information", is also relevant as some statutes require the presentation or production of "originals", other than for evidential purposes. The Evidence Code will resolve issues involving the admissibility of electronically generated information as evidence in a court proceeding.[229]

### *Requirements for "originals" in New Zealand legislation*

124 There are various provisions in legislation which impose requirements for supplying, depositing, and receiving *original* documents. With the exception of the Insurance Companies' Deposits Act 1953, the Insolvency Act 1967, the Income Tax Act 1994, the Patents Amendment Act 1992, and the Archives Act 1957, all of

---

[228] In this chapter we have limited our discussion to how statutory requirements for record keeping can be met electronically. However, we note that businesses create and store records electronically for much wider reasons: "The e-commerce revolution is causing the amount of data to explode, and people are looking for control of both the data, in a management sense, and also access to the information . . . in a performance sense" (S Burke of IBM in A Wells "IBM's shark set to look into data management" in *Infotech Weekly*, 1 August 1999, 7).

[229] See discussion in chapter 7, Evidence.

these provisions contemplate that the requirements can be fulfilled in respect of copies of the documents, as long as these are properly certified in accordance with the particular statute.

### *Examples*

- The Arbitration Act 1996, Schedule 1 article 35(2) provides that the party relying on an award or applying for its enforcement shall supply the duly authenticated *original* award or a duly certified copy.[230]
- The Archives Act 1957 section 9 provides that where any public archive or public record is in the possession of any person other than a government office, and the *original* of that archive or record is not in the possession of any government office, that person shall deposit that archive or record in the National Archives.
- Regarding the admissibility of banking records, section 47B of the Evidence Act 1908 provides inter alia that where a record is of information recorded or stored in written form, that the copy has been compared with the *original* entry or with a copy made in accordance with section 156A (4) of the Reserve Bank of New Zealand Act 1989 and is correct.
- Under the Goods and Services Tax Act 1985 section 24(1) a supplier must provide the recipient at his/her request with a tax invoice, and if the supplier claims to have lost the *original* tax invoice, s/he may provide a copy marked "copy only". The same applies in section 25(3) in respect of credit notes.
- Under the Hire Purchase Act 1971 section 7(1)(d) a copy of the hire purchase agreement marked "Purchaser to keep this copy" shall be given to the purchaser at the same time as the *original* is given for execution, if the purchaser executes the agreement on a day later than the other party.
- Section NF11(6) of the Income Tax Act 1994 provides that anyone who is required to deliver up a certificate of exemption must deliver up all *original* copies issued to them by the Commissioner.
- Section 127(4)(a) of the Insolvency Act 1967 provides a bankrupt is deemed not to have kept a proper record of transactions if s/he has not preserved a record of all goods purchased in the course of business, duly supported by *original* invoices.

---

[230] See also articles 4(1) and 6(1).

- Section 16(7) of the Insurance Companies' Deposits Act 1953 requires the *original* of each annual statement to be signed by the auditor and so on.
- Sections 58 and 62 of the Partnership Act 1908 provide that in cases of renewal or dissolution of a partnership, a certificate must be signed in a like manner as the *original* certificate.
- The Patents Amendment Act 1992 enacts the Patents Co-operation Treaty, rule 92.4(d) of which provides any national Office or intergovernmental organisation may require the *original* of any document transmitted by telegraph, teleprinter, facsimile or other like means of communication producing a printed or written document to be furnished within 14 days of the earlier transmission.
- Section 152(4) of the Tax Administration Act 1994 provides that where the original of a record is in the custody or control of the record holder, a copy shall be admissible in evidence, provided that proof that it is a correct copy is given by someone who has examined the *original* record. Section 152(5) provides that where the record holder does not hold the original but only a purported copy, a copy of that copy may be admissible if the purported copy was made in the regular course of business and the copy of that copy is correct (both of which must be proved).

125 In addition many statutes provide that in legal proceedings copies of documents shall be admissible in evidence as of equal validity with an original document. These copies must also be certified in accordance with the requirements for each statute. For example, section 29 of the Charitable Trusts Act 1957 requires copies or extracts to be certified under the hand and seal of the Registrar of Incorporated Societies.[231]

### *Statutory requirements for record keeping*

126 As noted in ECom 1,[232] statutory requirements for record keeping are numerous. Company and tax legislation generally require

---

[231] See also, Companies Act 1993 s 363, copies or extracts from registered documents must be certified by the Registrar of Companies. Similar provisions abound in the Building Societies Act 1965 s 129, Customs and Excise Act 1996 ss 164–166, Designs Act 1953 s 32, Energy Resources Levy Act 1976 s 33, Goods and Services Tax Act 1985 s 30, Land Transfer Act 1952 s 45, Life Insurance Act 1908 s 27, Tax Administration Act 1994 ss 110 and 118, and the Trade Marks Act 1953 s 69.

[232] ECom 1, para 391.

records to be retained for at least seven years, and there are penalties for non-compliance.[233] For example, section 190 of the Companies Act 1993 permits records to be kept in written form or ". . . in a form or in a manner that allows the documents and information that comprise the records to be easily accessible and convertible into written form". The company must also ensure that adequate measures are in place to prevent records from being falsified and to enable any alteration to be detected.

127 Submissions made to the Law Commission strongly supported the introduction of article 10 or an equivalent. However the New Zealand Law Society entered the following caveat:

> it does not necessarily provide adequately for those people or organisations who wish to save electronically the information from other records (in paper or other electronic formats). In that case, while the electronic information may be available it will at best be only a copy of the original record. The individual requirements for retaining records will need to be considered before there can be a move to eliminate the original records and rely entirely on electronic copies.[234]

In other words, the concern is that if the law required that an original paper document be retained, it may not be satisfied by the retention of an electronic record.

128 This problem highlights the fact that different types of records raise different issues regarding their retention. There are those created and maintained in electronic systems, and those created in paper and converted to electronic form. This distinction was observed in the final report of the Victorian Electronic Records Strategy,[235] in the context of the admissibility of electronic records as evidence. It was also noted in ECom 1,[236] that electronically generated information does not have an "original" in the sense in which that term is generally understood in the law of evidence. If "original" is defined as the medium on which information is fixed for the first time, it would not be possible to speak of "original" data messages, since the addressee of a data message would always receive a copy thereof.[237]

---

[233] Generally, see Companies Act 1993, s 87, Goods and Services Tax Act 1985, s 75 and Land Transfer Act 1952, s 33.

[234] New Zealand Law Society submission, 15 February 1999, 9.

[235] Public Record Office, Victoria, Australia 1998.

[236] ECom 1, para 196.

[237] Guide to Enactment, para 62.

129 Article 8 provides that any requirement to present or retain information in its original form is met by retaining a data message provided there is a reliable assurance as to the integrity of the information, and that if the information is required to be presented to a certain person, then it is capable of being displayed to that person. The Guide to Enactment informs us that article 8 is intended to cover documents which must be transmitted in "original" form (for example, weight certificates, inspection reports, insurance certificates) as well as documents of title and negotiable instruments. The Guide observes that the advantage of sending an original paper document is that other parties may be confident that the content has not been altered. So long as the *integrity* of the data message can be assured from the time it was generated, then the functional equivalent of originality is met by the data message.

130 The Australian Bill implements article 10 in clause 12. Clause 12 specifies that the electronic form of a document must be "readily accessible so as to be useable for subsequent reference", and must maintain the integrity of the information. "Readily accessible" is intended to mean that the information contained in the electronic communication should be readable and capable of being interpreted. "Useable" is intended to cover use by both humans and machines, and means more than mere receipt of a data message. These terms are more fully explained in the Explanatory Paper issued by the Attorney-General's Department.[238] Clause 12(1)(a) specifies that the document must satisfy these requirements "at the time of the recording of the information", which avoids inadvertently requiring a stored communication to be updated so as to be retrievable every time technology changes. The integrity of the information requirement relates to the method of generating a document in electronic form. Relevant matters in determining whether the method is reliable include:

- methodical recording of the information;
- assurance that the information has been captured without omission; and
- protection of the information against alteration.

131 Clause 12 deals with the retention of written communications separately from retention of electronic communications. The requirements in respect of each are the same, except for an additional requirement for electronic communications that information

[238] Available at http://www.law.gov.au/ecommerce/.

identifying the sender and recipient of the communication and the time when it was sent and received must also be retained.

132 Clause 11 of the Australian Bill is based on article 8 of the Model Law, with some differences. It provides that requirements and permissions to "produce" documents will be met by producing a document in electronic form, subject to conditions regarding accessibility and integrity of the information. The Explanatory Paper considers that the "production" of documents is a more appropriate term than the concept of an original document. Clause 13 provides that exemptions from clauses 11 and 12 may be made by regulation, and that those clauses do not affect the operation of the Commonwealth Evidence Act 1955 or any common law rule of evidence. Both clauses 11 and 12 provide that copyright in a document will not a breached simply because it has been generated in electronic form for the purposes of those clauses.

133 The hallmarks of existing New Zealand legislation which permit manual records to be kept in electronic form are:

- the records must be easily accessible;
- the records must be easily convertible into written form;
- there must be adequate measures in place to prevent records from being falsified and allow alterations to be detected.[239]

134 Similar themes are to be found in both articles 8 and 10 of the Model Law. Under article 8 there must be a reliable assurance as to the integrity of information from the time it was first generated in its final form; under article 10 the information must be accessible, usable for subsequent reference and in a format which can be demonstrated to represent accurately the information generated, sent or received.

135 We have considered whether adoption of a provision akin to recent New Zealand legislation (for example section 190 of the Companies Act 1993) within our proposed Electronic Transactions Act would remove barriers to electronic commerce adequately. We consider it preferable to adopt provisions akin to clauses 11 and 12 of the Australian Bill. We have come to this view for the following reasons:

- Section 190(1)(b) of the Companies Act 1993 requires information to be "convertible into written form" whereas the Model Law and the Australian Bill concentrate on a requirement of "usable for subsequent reference" which is broader and more enabling in nature.

---

[239] For example, Companies Act 1993, s 190.

- Section 190(2) of the Companies Act 1993 provides that there must be adequate measures to prevent and detect falsification of records. The threshold is lower than the Model Law and the Australian Bill in their respective requirements to "represent accurately" the information generated, and provision of a reliable means of assuring the maintenance of the "integrity of the information". The Companies Act provision may not cover an alteration which did not amount to falsification. In comparison, clause 12(3) of the Australian Bill ensures that properly endorsed changes and insignificant changes will not negate "the integrity of the information".

136 Article 8 of the Model Law and clause 11 of the Australian Bill address requirements to present or retain original information. As noted previously, the Explanatory Paper to the Australian Bill considers that "production" of documents is a more appropriate term.[240] Clause 13 of the Australian Bill exempts clauses 11 and 12 from the operation of the (Commonwealth) Evidence Act 1955 or any common law rule of evidence. In our view, an equivalent clause 11 of the Australian Bill is required to cover documents which must or may be produced outside of legal proceedings. Examples of such documents include documents of the type to which we refer in paragraph 129.

137 On the assumption that the Evidence Code is enacted contemporaneously with the proposed Electronic Transactions Act, we recommend that the equivalents of clauses 11 and 12 of the Australian Bill expressly state that they do not affect the operation of the Evidence Code or any common law rule of evidence. Alternatively, this could be stated in a separate provision akin to clause 13 of the Australian Bill.

138 Finally, we refer back to the question of certified copies to which reference was made earlier.[241] In our view, electronic certification should be possible through the electronic signatures regime we propose.[242]

---

[240] See para 132. An example of a requirement to produce information from a New Zealand statute is s 206(1)(b) (not yet in force) of the Fisheries Act 1996 which gives powers to Fisheries Officers to require information to be reproduced in a useable form.

[241] See paras 124–125.

[242] See chapter 9, Electronic Signatures, paras 153–155.

# 9
# Electronic signatures

139 In ECOM 1 we examined the concept of an electronic signature and the legal definition of what constitutes a signature. We also considered the various uses of manual signatures and examined legislation passed in several jurisdictions to implement an electronic signature infrastructure.[243] We raised four questions for submissions:

- Question 14: Should New Zealand adopt a statutory provision similar to article 7 of the Model Law, which allows electronic signatures to have the same effect as manual signatures?
- Question 15: Should any such reform, if adopted, also specify acceptable standards for electronic signatures, or should standards of security or reliability be left for the market to develop?
- Question 16: Does New Zealand need a domestic electronic signature infrastructure?
- Question 17: Should the State play any role in facilitating the use of electronic signature technology, for example, by assuming responsibility for the implementation of such an infrastructure?

140 One of the options which we raised was the possibility of defining the term "signature" in the Interpretation Act 1999 in a manner consistent with the thrust of article 7 of the Model Law. Under article 7, the elements of the functional equivalent to a signature are the need:

- *to identify the person* and to indicate *that person's approval* of the information contained in the data message; and
- for the *method to be as reliable as was appropriate* for the purpose for which the message was generated or communicated.[244]

141 Article 7 only applies where a signature is a requirement of law. Where a signature is not required by law then the normal rules in relation to proving an agreement apply.

---

[243] See ECom 1, chapter 7.

[244] Generally, see ECom 1, paras 316–320 and 344–345.

142 Submissions commenting on electronic signatures were received from Kensington Swan, New Zealand Post, the Information Technology Association of New Zealand (ITANZ), the Ministries of Commerce and Consumer Affairs, the New Zealand Law Society, Telecom, the New Zealand Bankers Association and the Government Communications Security Bureau (GCSB). Not all submitters made comments on each of the four questions.

143 In relation to question 14, it was agreed that electronic signatures should have the same effect as manual signatures, that statutory reform is necessary and that minimalist, technology-neutral legislation should be adopted. The great majority of submissions favoured legislating along the lines of article 7 of the Model Law.

144 In relation to question 15, submitters were of the general view that legislation should not specify acceptable standards for electronic signatures. The majority of submitters felt that standards of security and reliability should be left for the market to develop. Many submitters were of the view that one form of electronic signature technology would be unfairly advantaged if legislation specified technical standards; it was noted that adverse economic consequences for New Zealand businesses could result if prescribed standards were quickly superseded. It was also submitted that prescribing standards would be contrary to the principle of technological neutrality. Several submissions argued that any specification of standards would restrict rather than extend the range and application of the law. However, a number of submitters argued that some standards are necessary. For instance, the GCSB was of the view that there is a need to establish a standard for electronic signatures so as to facilitate their widespread use. To do otherwise was thought to result in a proliferation of systems, which might lead to incompatibility between those systems and a consequent impediment to their use.[245]

145 In relation to question 16, submitters agreed unanimously that there is a need for an electronic signature infrastructure. All of the submitters were of the view that State intervention and regulation is not required and that the private sector can develop an adequate infrastructure. Many submitters argued that establishing an electronic signature infrastructure is not a matter which requires law reform.

146 In relation to question 17, all of the submissions received were against the State assuming responsibility for the implementation

[245] GCSB submission, 24 November 1998.

of an electronic signature infrastructure. Submitters considered that the State should only play a minimal role in facilitating the use of electronic signature technology. It was generally agreed that the State's role in encouraging the use of electronic signature technology should be limited to enacting legislation making electronic signatures equivalent to manual signatures.[246]

## OVERSEAS DEVELOPMENT SINCE ECOM 1

147 We set out, in appendix E, a summary of developments which have taken place overseas since publication of ECom 1. Those developments are limited to national laws and the European Commission Directive. The purpose of the summary in appendix E is to identify the way in which other States are approaching electronic signature legislation.

148 In February 1999, the UNCITRAL Working Group on Electronic Commerce held its 34th working group session. The Working Group considered the work which had been undertaken by UNCITRAL in relation to electronic signatures.[247] The report of the Working Group on the work of its 34th session[248] instructs the Secretariat to prepare revised draft rules for consideration by the Working Group at a future session. A further session of the Working Group took place in Vienna from 6–17 September 1999.[249] It is conceivable that the Working Group will conclude its work in February 2000.

149 The work of UNCITRAL on electronic signatures is, we believe, of primary significance to New Zealand. For reasons which we will outline shortly, we recommend that article 7 of the Model Law be adopted into our proposed Electronic Transactions Act. Adoption of an equivalent to article 7 will enable a court to consider the

---

[246] New Zealand Post submitted that the State can play a useful role in the facilitation of electronic signature technology by enacting legislation, by becoming a supportive user of market driven techniques for electronic signature use, by becoming a user in a market driven infrastructure should one arise, and by being an advocate for the use of electronic signatures generally: New Zealand Post Limited submission, 17 December 1998.

[247] See Draft Uniform Rules on Electronic Signatures, Note by the Secretariat, Working Paper 79; Electronic Signatures, Note by the Secretariat, Working Paper 80 and Draft Uniform Rules on Electronic Signatures, Note by the Secretariat, Working Paper 82 (the Working Papers are available at UNCITRAL's website: www.uncitral.org).

[248] Available at www.eu.or.at/uncitral/english/sessions/unc/unc-32/acn9-457.htm.

[249] Because of publication deadlines this report was prepared prior to that session.

reliability of the electronic authentication device in determining whether a document should be regarded as "signed" for the purposes of specific legislation. As noted previously, this will involve questions of fact and degree. An email message from A to B purporting to guarantee the debt of C in the sum of $20 may well be regarded as acceptable by the court for that purpose, but a similar message guaranteeing a debt of $1,000,000 is not likely to be regarded as sufficiently reliable. Likewise, a simple email message is most unlikely to be regarded as sufficient to constitute a "signature" for the purposes of an agreement for sale and purchase of land to which section 2 of the Contracts Enforcement Act 1956 applies.

150 When the court assesses the "reliability" of an electronic equivalent to a manual signature, the risk of fraud being perpetrated will be one of the major factors considered. If a contract for the sale and purchase of land is entered into between two parties using accepted public key infrastructure (PKI) systems,[250] for which there is a certificate of verification available from a reputable company, that is likely to give weight to the view that the electronic signature is sufficient.

151 Any electronic signature regime must take account of the different levels at which business is done. For those involved in high value transactions or specific projects, particular contractual documents are likely to record fully the way in which parties will be bound when, for example, varying the terms of a contract. For small to medium sized enterprises engaging in electronic commerce over the internet, different considerations apply as one-off contracts will rarely be cost effective. Consumers entering into contracts over the internet are likely to be faced by standard form contracts imposed by persons with whom they deal who may be offshore.

152 The UNCITRAL Working Group on Electronic Commerce is currently reviewing questions of attribution of electronic signatures, the relationship between the proposed uniform rules and the Model Law, the definition and minimum qualities of certification authorities, cross-border recognition of certificates, and revocation and suspension of certificates.[251] In our view, the

---

[250] For a definition of the public key infrastructure see ECom 1, paras 322–323.

[251] One of the issues which will need to be addressed by UNCITRAL is the purpose of the proposed uniform rules. At present those uniform rules address party autonomy, the nature of the obligations which should be imposed on a person who holds a signature device, the person to whom such obligations should be owed and the obligations of the certification authorities.

question whether New Zealand should adopt more sophisticated electronic signature legislation should await the outcome of UNCITRAL's further work. If norms can be agreed among the States which contribute to UNCITRAL's work, then there may be merit in New Zealand going further and adopting legislation which deals with a higher level of electronic signature. New Zealand was represented at both the February 1999 and September 1999 UNCITRAL meetings by Paul Heath QC. Matters raised in submissions for ECom1 in relation to electronic signatures were put before the UNCITRAL Working Group meeting by the New Zealand delegate.

## RECOMMENDATION

153 We have come to the view that article 7 of the Model Law should be enacted into New Zealand law so that immediate barriers caused by statutory references to "signing" can be removed. This position was supported generally by the submissions made to us in response to ECom 1. The way article 7 is framed will allow the courts to exercise judgment in determining what type of electronic signatures can be used in lieu of a manual signature.[252]

154 We also recommend that no further action be taken in the meantime to deal with what we term "enhanced electronic signatures". By the term "enhanced electronic signatures" we refer to the electronic equivalent of manual signatures which are required to be enacted in a particular form and with more than just a physical signature from the person concerned.[253] In our view the question whether any further legislative action is required should await development of the work of the UNCITRAL Working Group on Electronic Commerce.

155 Submitters favoured a minimalist approach from Government and, to the extent that a detailed infrastructure for electronic or digital signatures was considered appropriate, leadership of such development by the private sector. Although some States have adopted prescriptive legislation designed to provide a framework within which the PKI for digital signatures can operate, it is our view that legislation of that type would both:

---

[252] See paras 140 and 149–150.

[253] For example deeds which are required to be witnessed by a person who adds his or her name, address and occupation: Property Law Act 1952 s 5.

- create a competitive advantage to those engaged in the provision of such services when other technologies (such as biometrics) may soon become available and cost effective; and
- be a breach of our technological neutrality principle.

Accordingly, we do not support the introduction of legislation of that type in New Zealand.

---

# 10
# Security and encryption

156 CRYPTOGRAPHY IS THE SCIENCE of transforming data into an unreadable form, in order to keep it secure when it is being transmitted or stored. Cryptography can also be used

- to prevent data from being modified; or
- to prevent data from being used without authority.

It can also authenticate or confirm the origin of an electronically generated message. Cryptography is an essential element of the public key framework used for digital signatures. We discussed encryption in ECom 1 in the context of digital signature technology.[254]

157 In the context of electronic commerce, cryptography can be a valuable tool for ensuring that business communications are kept confidential and secure. Once data is encrypted its contents can only be read by persons who have access to the secret key necessary to decrypt it. Thus, the need for sensitive commercial communications to be kept confidential and the desire to keep personal information secure can be met through the use of cryptography.

158 An issue arises as to the right of law enforcement and intelligence and security agencies to gain access to the key or code required to decrypt messages. This issue is of no little complexity as it raises the fundamental questions about the balance to be struck between rights of privacy and business confidentiality (on the one hand) and the public interest in investigating and detecting crime and threats to national security (on the other hand).[255]

159 Since our first report was published, the Government has established an interdepartmental National Cryptography Policy Committee to make recommendations for consideration by Government. The Committee is taking into account the OECD

[254] See ECom 1, chapter 7, Electronic Signatures, paras 322–324.

[255] ECom 1, paras 349–352.

Guidelines for Cryptography Policy,[256] which establish a broad framework, to be reviewed every five years, and which are based on principles of trust, choice, private sector leadership, industry standards, privacy, lawful access, accountability and international cooperation.

160 We are advised that the National Cryptography Policy Committee may recommend that New Zealand take an approach consistent with that of our major trading partners. The National Cryptography Policy Committee plans to publish a consultation document following initial consideration of issues by Cabinet. Public submissions will be sought.

161 The National Cryptography Policy Committee may make recommendations to Government on whether, and if so in what circumstances, law enforcement and intelligence and security agencies should be able to obtain the key required to decrypt private messages, once it has obtained submissions from the public in response to the policy document it proposes to publish. We note that the difficulty in compelling a person to disclose the means of decryption, or the plain text of the document itself, will need to be given considerable thought; as will the question of an appropriate sanction in the event that disclosure is not made. In that regard, the disclosure of something held in one's head is somewhat different in kind to the provision of DNA samples under the Criminal Investigations (Blood Samples) Act 1995.[257] Ultimately, any view formed on this issue will need to recognise that a private key may be held in the memory of a human being, rather than located in an electronic or paper based record.

## EXPORT OF ENCRYPTION PRODUCTS

162 While the manufacture, use and import of strong encryption is not regulated in New Zealand, there are some controls over the export of these products. These reflect New Zealand's obligations under the Wassenaar Arrangement, which is an agreement between 33 countries[258] setting guidelines for the cross-border flow of dual

---

[256] Available from the OECD website: http://www.oecd.org//dsti/sti/it/secur/prod/e-crypto.htm.

[257] See in particular Criminal Investigations (Blood Samples) Act 1995 s 54(2).

[258] Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovak Republic, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom and United States.

purpose goods and technologies of strategic significance.[259] The relevant cryptography portion of the Arrangement is valid until December 2000 and is contained in Category 5 Part 2. The availability of strong encryption in this country is arguably enhanced by our belonging to the Arrangement, as other exporting countries will be more likely to trust New Zealand importers as end-users.[260]

163 Part IV of the Second Schedule to the Customs Export Prohibition Order 1996 provides that certain conventional weapons, and other goods with dual applications including military use, are not to be exported from New Zealand. A list of these exports can be obtained from the Ministry of Foreign Affairs and Trade (MFAT). Currently anyone wanting to export strong encryption software must apply for a licence for each export from MFAT. While these licences are normally granted within 48 hours of application,[261] this policy has been criticised for being cumbersome and stifling commercial dealings in this area.[262]

164 We make no specific comments on this issue as the National Cryptography Policy Committee will refer to the question of export of encryption products in its public discussion paper. 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.

---

[259] See www.wassenaar.org to read the text of the Arrangement.

[260] See comments by J Higgins in K Griggs "Cold War protocol risks e-commerce" *National Business Review* 12 February 1999, 6.

[261] Ministry of Foreign Affairs and Trade *New Zealand's Controls on the Export of Strategic Goods* (Wellington, November 1996) 2.

[262] Above n 260.

# 11
# Privacy

165 In a recent article, the Hon Justice Michael Kirby stated:

> The speed, power, accessibility and storage capacity for personal information identifying an individual are now greatly increased. Some of the chief protections for privacy in the past arose from the sheer costs of retrieving personal information; the impermanency of the forms in which that information was stored; and the inconvenience experienced in procuring access (assuming that its existence was known). Other protections for privacy arose from the incompatibility of collections with available indexes and the effective undiscoverability of most personal data. These practical safeguards for privacy largely disappear in the digital age. A vast amount of data, identified to a particular individual, can now be collated by the determined investigator. The individual then assumes a virtual existence which lives in cyberspace instead of in what is sometimes described as "meat space". The individual takes on a digital persona made up of a collection of otherwise unconnected and previously unconnectable data.[263]

166 And in a paper presented to the APEC Steering Group on Electronic Commerce, the Privacy Commissioner noted:

> It is interesting to consider why, in a consumer age where quality, choice and convenience is demanded, the level of e-commerce is so low. One reason is the appeal of conventional shopping. Another is a lack of consumer confidence in doing business electronically . . . They worry about the security of their personal information and fear it may be misused. Information privacy concerns are discouraging consumers from using the Internet to buy goods and services . . .
>
> Private ownership of personal computers continues to increase, and the online consumer market is growing exponentially. However, a recent survey in the US found that only 23% of computer users with Internet access said they already paid for information or purchased products online . . . The reasons seemed to be privacy focused. A clear majority of people were concerned about threats to their personal privacy while on line. . . . it was clear from the survey that a lack of

[263] Hon Justice Michael Kirby "Privacy in Cyberspace" (1998) 21(2) UNSW Law Journal 323, 325.

privacy protection was deterring people from using the Internet and e-commerce. Of those who were not likely to access the Internet in the next year, greater privacy protection was the factor that would most likely convince them to do so.[264]

## OVERSEAS LEGISLATION

167 New Zealand's privacy legislation (the Privacy Act 1993) goes further in protecting an individual's privacy than many of our major trading partners.[265]

168 In the European Union (EU), privacy law 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.[266] The Directive was adopted on 24 October 1995. The Directive sets out a number of principles in relation to the collection, processing and accessing of personal data. The data protection principles include: personal data must be processed fairly and lawfully; collected for specified purposes; accurate and kept up to date; processed only if the subject has given consent; individuals from whom information is collected have the right to access the data and adequate security measures

---

[264] Office of the Privacy Commissioner "Privacy Protection: The Key to Electronic Commerce", seminar delivered at Asia -Pacific Economic Cooperation Conference, Auckland, 27–28 June 1999, 1–4.

[265] The Privacy Act 1998 (Commonwealth) is the primary piece of domestic legislation relevant to information privacy protection in Australia. The Privacy Act confers on individuals enforceable rights in respect of their "personal information" (defined in section 6(1)) against Commonwealth government departments and agencies. It has however recently been reported that the Australian government will be enacting new laws on information privacy which will also cover the private sector (see Electronic Commerce Report, 25 January 1999, 3). Canada has privacy legislation at the commonwealth level. The Privacy Act (chapter P-21) applies to government institutions and provides a number of rules in relation to the collection, retention and disposal of personal information. On 26 October 1999 the Personal Information, Protection and Electronic Documents Bill was passed by the Canadian House of Commons, and was due to receive its second reading in the Senate at the time of publication of this report. The Bill applies to every "organisation" in respect of "personal information" collected, used or disclosed by the organisation in the course of commercial activities (s 4). "Organisation" is defined as including an association, a partnership, a person and a trade union and "personal information" is defined as meaning information about an identifiable individual (s 2). The Bill requires every organisation to comply with the obligations set out in schedule 1 (s 5). Schedule 1 sets out the protection of personal information principles.

[266] Available at http://www.privacy.org/pi/intl_orgs/ec/final_EU_Data_Protection.html.

must be used to safeguard the personal information. Article 25 requires Member States to provide that the transfer to a third country of personal data may only take place if the third country has an "adequate level" of privacy protection and article 32 requires Member States to bring laws necessary to comply with the Directive into force prior to October 1998.

169 In the United Kingdom the Data Protection Act 1998 implements the EU Data Protection Directive. The Act requires data controllers to comply with a set of data protection principles in relation to personal data processed by the data controller (section 4). The following rights for data subjects are established in the Act: the right of access to personal data (sections 7 to 9); the right to prevent processing likely to cause unwarranted damage or distress (section 10); the right to prevent processing for purposes of direct marketing (section 11); rights in relation to automated decision-taking (section 12); compensation for failure to comply with certain requirements (section 13); and also rights in relation to rectification, blocking, erasure and destruction of inaccurate data (section 14). Also, principle 8 provides that personal data must not be transferred to a country or territory outside the European Economic Area (which is made up of the 15 EU nations plus Iceland, Liechtenstein and Norway) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

170 New Zealand's privacy law is governed by the Privacy Act 1993. In discussing the Privacy Act 1993, the Privacy Commissioner has recently said:[267]

> If privacy is the key, then New Zealand consumers have an advantage – at least when they deal with New Zealand-based businesses. In New Zealand, consumers' privacy concerns can largely be met through businesses complying with the Privacy Act. When properly applied, the Act's emphasis on purpose and openness tends to allay consumers' concerns about what might happen to their information. A legal requirement to maintain reasonable security safeguards reassures consumers about the security of their information – and that they have a practical remedy to pursue. The availability of a complaints mechanism gives confidence that promises of respect for their personal data can be enforced (1–2).
>
> . . .
>
> Any business based in New Zealand wishing to engage in e-commerce with consumers must ensure its activities comply with the Privacy

[267] See n 264.

> Act, to the extent that they involve personal information about their customers.
>
> The Privacy Act applies to the handling of all personal information collected or held by agencies, whether in the public or private sectors. Although there are some minor exceptions, all businesses from sole traders to multi-national conglomerates with a New Zealand branch are covered by the Act.
>
> Personal information includes any information about an identifiable living person, whether it is on a computer, in a paper file or in someone's head (5–6).
>
> . . .
>
> Central to the Act are its twelve information privacy principles . . . the principles are technology neutral, which means they have the flexibility to operate in a number of contexts. It also means they will not date as new technologies come into existence (6).
>
> . . .
>
> New Zealand is fortunate in having a broadly based technology neutral privacy law that covers the public and private sectors. Hence, privacy law does not pose an obstacle to the development of e-commerce within New Zealand or for New Zealand business seeking consumer sales overseas (13).

171 The Privacy Act has a set of Information Privacy Principles which are applied in a broad range of circumstances. The principles apply to all "personal information" held by an "agency". "Personal information" means information about an identifiable living individual and "agency" is defined as meaning any person or body of persons, whether corporate or unincorporate, and whether in the public sector or the private sector (section 2). The Act is technology neutral[268] and applies to all personal information, whether it is held in electronic or manual form.

172 The Information Privacy Principles include:[269]

- personal information must be collected for a lawful purpose;
- personal information must be collected directly from the individual concerned;
- the individual must be made aware of a number of matters (including that the information is being collected, the purpose for which the information is being collected, the intended

---

[268] Office of the Privacy Commissioner "Review of the Privacy Act: A background paper" August 1998; Stewart "Information Security – Privacy Law and Issues" (1997) 2 HRLP 225.

[269] Privacy Act 1993 s6.

recipients of the information, and the name and address of the agency collecting the information);

- personal information must not be collected in an unlawful or unfair manner;
- personal information must be protected by adequate security systems;
- individuals are entitled to have access to, and request correction of, personal information held about them;
- personal information shall not be used unless it is accurate, up to date, complete, relevant and not misleading;
- agencies must not hold personal information for longer than is required; and
- personal information must not be used for any purpose other than that for which it was collected.

173 When a person believes that an action constitutes an interference with his or her privacy, the individual may complain to the Commissioner (section 67). The Commissioner may investigate the complaint (section 70) and if the Commissioner decides that the complaint has substance, the Commissioner must attempt to reach a settlement between the parties (section 77). If a settlement is not reached, civil proceedings before the Complaints Review Tribunal may be taken (section 82). The Complaints Review Tribunal may grant a declaration that the action interfered with the privacy of the individual, make an order restraining the defendant from continuing or repeating the interference, award damages, or make an order that the defendant perform any act specified in the order (section 85).

174 In his presentation to the APEC Steering Group on Electronic Commerce, the Privacy Commissioner argued that privacy law does not pose an obstacle to the development of e-commerce within New Zealand.[270] However, it is important to note the effect that article 25 of the EU Data Protection Directive[271] and principle 8 of the Data Protection Act 1998 (UK),[272] which prohibit the transfer of personal information to territories which do not have "adequate" privacy protection laws, may have on electronic commerce in New Zealand. The Privacy Commissioner has recently noted the importance of the EU Data Protection Directive for electronic commerce. In the Privacy Commissioner's view, the

---

[270] See para 170.

[271] See para 168.

[272] See para 169.

impacts of the EU Data Protection Directive will increasingly be felt over the next few years:

> The crux of the Directive for businesses outside Europe is its limitation on the transfer of personal information out of Europe except to third countries which ensure an adequate level of protection. This has the potential to impact significantly on businesses in this region handling personal information about EU residents for European companies. If a business is not in a jurisdiction with "adequate" privacy law, the Europeans may look to what sectoral laws or voluntary codes of compliance apply to the business. If there are none, the business may have to negotiate special contracts in order to carry out transactions with European consumers.[273]

175 The Privacy Commissioner has recently made a number of recommendations for amendment of the Privacy Act 1993.[274] Two of the amendments recommended are designed to ensure that the Privacy Act will be deemed "adequate" under the EU Data Protection Directive. First, the Privacy Commissioner recommends amendment to section 34 of the Privacy Act. Section 34 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. The Privacy Commissioner recommends that the denial of the right of access to non-New Zealanders who are not present in New Zealand at the time should be done away with.[275] Secondly, the Privacy Commissioner notes that there is a possibility that European agencies may divert data transmissions through New Zealand to another country so as to avoid the "adequacy" provisions in the EU Directive. The Privacy Commissioner recommends that this should be prevented.[276]

176 In his review of the Privacy Act 1993, the Privacy Commissioner also notes that the definition of "document" currently provided in the Privacy Act 1993 could be amended so that it is in conformity with the Evidence Code recommended by this Commission in 1999.[277]

---

[273] See n 264, 3.

[274] Office of the Privacy Commissioner *Necessary and Desirable: Privacy Act 1993 Review: Report of the Privacy Commissioner* (November 1998).

[275] See para 274, para 5.3 and recommendation 61.

[276] See para 274, recommendation 35(a).

[277] See para 274, para 1.4.71 and *Evidence: Reform of the Law: NZLC R55 vol 1* para 512–514; *Evidence: Evidence Code and Commentary: NZLC R55 vol 2* s 4, c13.

## The issues

177 We agree with the Privacy Commissioner that New Zealand needs to have effective privacy laws to encourage electronic commerce. We also agree that the Privacy Act 1993 applies adequately to the electronic environment. Further, for the reasons given by the Privacy Commissioner, we agree that the amendments to the Privacy Act 1993 which he recommends (discussed above) should be adopted.

178 We seek submissions on the issues arising from the process of "caching". The term "caching" is defined by Gringras[278] in the following way:

> Caching is when a server with vast storage capacity holds copies of the most popular pages on the worldwide web. If this web cache is located on the local area network users can be saved the delay of gaining access to overburdened sites.

This also means that information may be held on a personal computer and the owner of the computer has no knowledge about the information and no intention to collect the information. The Privacy Act 1993 has 12 principles, the first 11 of which may have implications in relation to caching. The first four deal with "collection" of personal information while the balance affect information held by agencies (whether collected directly or indirectly from an individual or otherwise generated or obtained). The term "collect" is defined to exclude "receipt of unsolicited information". There is an issue as to whether an agency involved in electronic commerce can be considered to be collecting information through caching. Further issues arise in relation to the retention, use and disclosure of such information and rights of individual access or correction if the information is readily retrievable.

179 We seek submissions in relation to the privacy issues raised by caching, and particularly as to:

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

---

[278] Gringas *The Laws of the Internet* (Butterworths, London, 1997) 380.

# 12
# Criminal law

180 COMPUTER MISUSE is a global issue. Statistics reveal that computer misuse has been occurring for several years and is a widespread problem. In 1995 the United States General Account Office discovered that hackers using the internet had broken into the US Defence Department's computer more than 160,000 times.[279] The Federal Bureau of Investigation reported that in 1997 there were 206 pending computer misuse cases. By 1998 that figure had increased to 480.[280]

181 The society in which we live is becoming increasing reliant on computers. In 1997 it was estimated that as many as 40 million people around the world were using the internet. It was predicted that this figure would rise to 200 million by 1999.[281] As our reliance on computers increases so too does the potential for computer misuse. One of the areas where computer misuse could be acutely felt is in the area of commerce. As we noted in ECom 1[282] business-to-business commerce over the internet reached an estimated US$8 billion in 1997, 10 times the 1996 total.[283] It has been estimated that electronic commerce will be worth US$1 trillion by 2002.[284] Massive financial losses have reportedly occurred overseas as a result of computer misuse. In 1995, the US Senate's Permanent Investigations Sub-committee reported that banks and corporations lost US$800 million from hackers in 1995 alone. Also, federal law enforcement agencies have estimated that thieves operating through computers steal more than US$10 billion worth of data in the United States annually.[285] Further, computers are relied on to perform vital functions in many sectors of our society. They are

---

279 *Computer Misuse NZLC R54*, para 26.

280 D Denning *Information Warfare and Security* (ACM Press, New York, 1999) 56.

281 *Computer Misuse NZLC R54*, para 2.

282 ECom 1, para 5.

283 Above n 282.

284 *Computer Misuse NZLC R54*, para 1.

285 *Computer Misuse NZLC R54*, para 28.

used to administer banking and financial systems, transport control systems, communication systems, hospitals and a variety of other complex operations. A person who gains unauthorised access to a computer can cause major disruption. Computer misuse can cause extensive economic loss, not only to an individual company but also on a nation-wide scale; it can put lives in danger.

182 In the late 1980s several countries investigated the need for the creation of criminal offences directed specifically at computer misuse as a result of concerns in relation to computer crimes. The Scottish Law Commission, the Attorney-General's Department of Australia and the Law Commission of England and Wales[286] recommended the adoption of criminal offences directed at computer misuse. These recommendations were followed and there is now legislation in the United Kingdom and Australia making computer misuse a criminal offence. Legislation has also been passed in Canada and Singapore.[287]

183 It has recently been brought home to New Zealanders that computer misuse is not just an overseas problem. In November 1998, a computer hacker erased some 4,500 "Ihug" websites. Shortly after the Ihug incident, it was reported that Telecom, New Zealand's largest Internet service provider, was concerned that hackers might be gaining access to the internet by using customers' passwords and surfing the internet at the customers' expense. At the same time as these incidents were occurring, the Law Commission was in the process of receiving submissions from the public and private industry on ECom 1. Many of the submissions received recommended that the Law Commission should address the issue of electronic crime.

184 We decided late last year to address the issue of computer misuse. In May this year we published our report *Computer Misuse* and provided a copy to the Ministry of Justice. In September this year the Crimes Amendment Bill (No 6) received its first reading in Parliament. Two computer misuse offences are contained in the bill; accessing a computer system for a dishonest purpose and damaging or interfering with a computer system. The offences contained in the bill are narrower than the offences recommended by the Law Commission in our report *Computer Misuse*.

---

[286] See *Computer Misuse NZLC R54* para 3 where these reports are discussed.

[287] See *Computer Misuse NZLC R54* appendix A where this legislation is reproduced.

185 We deal briefly with the question of the criminal law in this report because, having regard to what we have learnt since publication of ECom 1 in October 1998, we adhere to our view that there is a real need for consistent and harmonious legislation dealing with both criminal and civil aspects of the law relating to electronically generated information. Also, we are raising the possibility of the creation of a statutory tort[288] to provide compensatory remedies which may not exist under the current law. That discussion cannot take place sensibly without a brief reference to the criminal law. In addition, there is one point of elaboration which we wish to make on our *Computer Misuse* report.

## Computer misuse legislation

186 Originally, we had intended to issue our *Computer Misuse* report as a preliminary paper. Ultimately, the report was issued as a final report because, about a month before publication, the Minister for Justice announced his proposal to introduce into the House of Representatives legislation which would create criminal offences for certain types of computer crime.[289] Because of the imminence of the introduction of a Bill, we issued a final report which was confined to concepts and which did not include draft legislation. Our recommendations were intended to add to those made in December 1998 when we made recommendations which would enable Parliament to close a gap in the law exposed by the judgment of the Court of Appeal in *R v Wilkinson*.[290]

187 Since the issue of our *Computer Misuse* report we have had further discussions with our Electronic Commerce Advisory Committee. We have come to the view that a fifth offence is necessary; namely intentionally and without authority gaining access to data in a computer. That offence would be in addition to the *access* offence mentioned in *Computer Misuse*. For convenience, we state below the five new offences which we have recommended be created and add a short comment on questions of jurisdiction in relation to such offences.

---

[288] See chapter 13, the Law of Torts, paras 197–270.

[289] *Computer Misuse*, preface, ix.

[290] [1999] 1 NZLR 403 CA; see *Dishonestly Procuring Valuable Benefits: NZLC R51* (Wellington 1998).

## The offences recommended in *Computer Misuse*

188 The first offence is one of unauthorised interception of data stored in a computer. This is where a person eavesdrops so as to pick up information in the course of being transmitted to, or received by, a computer or intercepts the emanations from a computer and transforms those emanations into a useable form. To establish this offence the prosecution would be required to show: first, that the accused obtained unauthorised interception of computer data, and secondly that the accused *intentionally* intercepted the computer data. In our view, those who accidentally intercept computer data should not be subject to prosecution. The offence would be expressed so as to include instances where the attacker physically attaches an interception device to a computer or transmission device (such as telephone wires) as well as instances where the attacker places a device in proximity to such equipment.

189 The second offence is unauthorised access to data stored in a computer. This is where a person without authority, whether through physical or electronic means, accesses data stored on a computer. It is not appropriate to punish with criminal sanctions a person who accidentally or even carelessly accesses data. For example, in some cases individuals may gain unauthorised access to data by mis-dialling or by opening a programme which they did not intend to open. Consequently, the prosecution should be required to establish: first, that the accused gained unauthorised access to data, and secondly that at the time of access the accused had an intention to cause loss or harm or gain a benefit or advantage. The requirement of such an intent would mean that those who gain access simply to achieve the prize of access would not be criminally liable for their actions. However, if a person obtained unauthorised access without such an intent but then went on to cause damage through careless conduct, that person would be liable for the offence of "damaging computer data".[291]

190 The third offence is unauthorised use of data stored on a computer. The term "use" would cover two distinct types of activity. The first is where a person without authority gains access to data stored in a computer and then goes on to use that data in an unauthorised way (for example to commit fraud or theft). The second type of activity is where a person plays no part in gaining unauthorised access to data but, nevertheless, receives and uses the data in an unauthorised way. This second situation is akin to receiving rather than theft.

---

[291] See para 191.

191 The fourth offence is unauthorised damaging of data stored in a computer. "Damage" would cover the entire continuum from denial of data through to modification through to destruction of that data. This category would cover both the "direct" and the "indirect" damaging of data. By "indirect" damaging we mean, for instance, writing a harmful "virus" on to a computer disk intending that someone else will use the disk and thereby introduce the virus into a computer or entering a password or otherwise blocking legitimate users from being able to access data. It would be sufficient to prove first, that the hacker gained unauthorised access and secondly, that data was damaged as a result of the hacker's actions (whether intentional or careless).

192 The fifth offence, to which we refer in paragraph 187 above, is an alternative to the second offence which is concerned with unauthorised access to data stored in a computer.[292] In our view, the elements of this fifth offence should be that a person intentionally and without authority gains access to data stored in a computer.[293] Initially[294] we took the view that the addition of an intent to cause loss or harm to the person entitled to data or to some third party or to gain some form of benefit or advantage either personally or for a third party, was needed to complete an offence of unauthorised access. That was why our "access" offence was framed the way it was in the *Computer Misuse* report. We are now persuaded that that view was too narrow. The offence we now propose would 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 massive financial losses to the computer owner who has to conduct a full audit on the system to determine where in the system the hacker had been and whether, in fact, any damage had resulted. It may well be necessary for the computer owner to shut down the system while performing an audit and this would cause further ongoing losses. The potential for harm in such circumstances, and the consequent need for deterrence, was underestimated by us in our earlier report. We now recommend that an additional offence be created. However, we see this offence as being less serious than the other four offences recommended in

---

[292] See para 189.

[293] The words "data" and "computer" are intended to have the meanings assigned to them in paras 14 and 15 of *Computer Misuse*.

[294] See *Computer Misuse* para 13.

the *Computer Misuse* report and we take the view that it should have a maximum penalty of three years imprisonment.[295]

193 In relation to the penalties for the other four offences we recommended that a single maximum penalty of 10 years imprisonment should be set for all four categories of computer misuse. It would then be up to the court to exercise a discretion on sentencing to fit the circumstances of the particular case.[296]

194 In the *Computer Misuse* report we also recommended that a provision giving New Zealand courts jurisdiction in computer misuse offences wherever they are committed should be enacted. We are of the view that the existing jurisdiction provisions in the Crimes Act 1961 are inadequate to deal with computer misuse

---

[295] In the report of the Crimes Consultative Committee on the Crimes Bill 1989 it is recommended that there should be an offence for access simpliciter. The Committee stated:

> [unauthorised access simpliciter] . . . may in fact have quite serious effects. Hacking may force owners of computer systems who become aware of a hacker's activities to engage in expensive and time-consuming efforts to check the extent of any intrusion and whether damage has been done.
>
> The Committee considers that criminal liability for simple unauthorised access would be appropriate provided the maximum penalty is set at a much lower level than for the offences in clauses 200 and 201. The Crimes Act should be reserved for serious offences. We suggest the location elsewhere of a summary offence dealing with unauthorised access, punishable by a maximum of six months imprisonment. (Crimes Consultative Committee, *Crimes Bill 1989, Report of the Crimes Consultative Committee* (April 1991) 77)

Taking into account the recommendations of the Crimes Consultative Committee and the fact that the prosecution does not need to establish an intention to cause loss or gain a benefit, we agree that the penalty for the fifth offence should be less than the penalty for the other computer misuse offences. We are, however, satisfied that the maximum penalty recommended by the Crimes Consultative Committee in 1991 is inadequate for today's purposes. There have been massive developments in computer technology and use since the Crimes Consultative Committee reported almost a decade ago. The potential for harm, and the consequent need for deterrence, has increased. We therefore recommend that the offence of intentionally and without authority gaining access to data stored in a computer should be located in the Crimes Act 1961 and should have a maximum penalty of three years imprisonment.

[296] In New South Wales a computer hacker recently appealed his three year sentence on the basis that the sentence was excessive. The New South Wales Court of Criminal Appeal dismissed the appeal on the basis that computer crime is a fast growing offence and offenders should expect substantial sentences (see (1999) 73 ALJ 394).

activities. Also, in many cases it will be impossible to determine where the hacker was at the time the computer misuse activities took place.

195 It is in the context of these recommendations that we discuss, in chapter 13, the question of whether there should be an additional statutory tort which would enable a person whose computer system had been entered illegally in one of the five ways set out above to sue for compensation for losses suffered or to receive back any profit gained by the person responsible for the hacking.[297]

## Future work

196 While preparing our report on computer misuse, it became clear to the Commission that computer misuse is an international problem which has no regard for territorial boundaries. In our view it is inadequate that States deal with issues of computer misuse in an isolated and piecemeal fashion. Rather there is a need for international initiatives in this area to ensure that States legislate to criminalise computer hacking (i) affecting those within its borders (wherever it is committed) and (ii) committed within its borders (wherever its effects may be). The Law Commission has decided to undertake further work on the issue of international measures for computer misuse over the coming year.

---

[297] See chapter 13, paras 197–270.

# 13
# The law of torts

197 In ECOM 1 we analysed how various tortious remedies applied to the electronic environment. After discussing the general nature of the law of torts,[298] we dealt separately with the torts of trespass to property,[299] breach of confidence,[300] negligence[301] and defamation.[302] We then 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.[303] Our provisional view was that it would not be feasible to introduce legislation because of the difficulty in articulating restrictions in a sensible and workable manner.[304] The great majority of submissions received supported that view for the same reasons that courts refuse to constrain the tort of negligence: circumstances in which the tort may need to be invoked in the future cannot readily be predicted.[305]

---

[298] ECom 1, paras 138–146.

[299] ECom 1, paras 147–157.

[300] ECom 1, paras 158–166.

[301] ECom 1, paras 167–185.

[302] ECom 1, paras 186–190.

[303] The only question posed in ECom 1 was:

> Are there any policy reasons for limiting the boundaries of tortious liability incurred from the use of electronic communication networks, having regard to the problems of defining "neighbourhood" in an electronic environment?

ECom 1, paras 191 and 192; submissions were sought in the context of the "floodgates principle" as a mechanism of limiting the boundaries of the law of tort.

[304] ECom 1, para 192.

[305] Not one submission received supported restriction of the tort of negligence through statutory intervention. Many submitters expressly endorsed the approach to the tort of negligence which has been developed in New Zealand; ie as based on the decision of the House of Lords in *Anns v Merton London Borough Council* [1978] AC 728; see also ECom 1, para 168.

198 Of more concern to those persons making submissions on the torts chapter was the need to clarify the liability of Internet Service Providers (ISP) for acts or omissions of their subscribers. Submissions underscored the view that too much uncertainty surrounds the issue of ISP liability. Different views were put forward as to the means of clarifying liability.

199 We have come to the view that it is appropriate to clarify the basis of ISP liability in the interests of ensuring that the law is as predictable as possible in this area. We address the reasons for our views at paras 240–261.

200 Although unconnected with the points made in submissions, it has also become clear to us that we need to address the interrelationship between the criminal law and the law of torts[306] to investigate whether there are any significant gaps in the law's protection of information which has been wrongfully obtained. We deal with this issue first.

## THE VALUE OF INFORMATION

201 We agree with the view of Fitzgerald that:

> . . . the fundamental premises of the new society include the notion that information is currency, there is an intangible delivery of products, there is non-territorial and decentralised nature to the way we do business. Time, space and physicality disappear into the background . . . information needs to be freely available to ensure social and cultural prosperity.[307]

202 We said in our *Computer Misuse* report that

> It is necessary to ensure that computer systems are not used to cause harm to others. Computers are relied on to perform vital functions in many sectors of our society. They are used to administer banking and financial systems, transport control systems, communication systems, hospitals and a variety of other complex operations. A person who gains unauthorised access to a computer can cause major disruption. Computer misuse can cause extensive economic loss, not only to an individual company but also on a nation-wide scale; it can put lives in danger. Unauthorised interference with an airport control system or computers in a hospital are examples of the latter.[308]

---

[306] See chapter 12, Criminal Law, and *Computer Misuse: NZLC R54* (Wellington, 1999).

[307] B Fitzgerald "Computer Software: Sales, Licences and Consumer Protection" (in the 1999 Fay, Richwhite Conference, Auckland, 1999) 5–6.

[308] *Computer Misuse: NZLC R54* (Wellington, 1999) para 35.

We then asked whether the time had come to redefine "information" as a property right for both civil and criminal law purposes.[309] We said:

> It is necessary to protect commercial information which may be of immense value. For many businesses operating in this environment, the information which is stored on their computer will be its most valuable commodity. It is important to recognise and protect the intellectual capital of information stored on a computer. The importance of *information* as a business asset in the *knowledge economy* may justify redefinition of *information* as a property right for both civil and criminal law purposes. In essence, it is both the *information* and the *systems* which we are proposing to protect in our recommendations in this report. The question whether information should be regarded as a property right for civil law purposes will be addressed further in the second Electronic Commerce report . . .[310]

203 The United States is, by far, the country whose citizens constitute the biggest number of users of the internet in the world. New Zealand, in 1996, had 200,000 users of the internet and a projected number of users for the year 2000 of 700,000.[311] This compares with the 1996 estimated number of United States internet users of 47 million.

**Figure 13.1: Estimates of internet users by country:1996–2000 (millions)***

| Country | 1996 | 2000 |
|---|---|---|
| USA | 47.0 | 65.0 |
| Japan | 6.7 | 32.0 |
| United Kingdom | 0.6 | 11.0 |
| Germany | 0.8 | 8.5 |
| France | 0.8 | 7.3 |
| Spain | 0.5 | 3.5 |
| Italy | 0.3 | 2.8 |
| Australia | 1.0 | 5.3 |
| Taiwan | 0.6 | 3.4 |

*continued*

[309] *Computer Misuse: NZLC R54* (Wellington, 1999) paras 21 and 36.

[310] *Computer Misuse: NZLC R54* (Wellington, 1999) para 36.

[311] Department of Foreign Affairs and Trade *Putting Australia on the New Silk Road* (Canberra, 1997) 12.

| Country | 1996 | 2000 |
|---|---|---|
| Republic of Korea | 0.2 | 2.9 |
| South Africa | 0.3 | 1.5 |
| Israel | 0.2 | 1.0 |
| China | 0.1 | 2.7 |
| Malaysia | 0.1 | 1.8 |
| India | 0.04 | 1.8 |
| Singapore | 0.2 | 0.9 |
| New Zealand | 0.2 | 0.7 |
| Thailand | 0.1 | 0.6 |
| Hong Kong | 0.2 | 0.7 |
| Indonesia | 0.1 | 0.6 |
| Philippines | 0.04 | 0.4 |
| Others | 3.0 | 14.0 |
| Total worldwide | 67.5 | 168.2 |

**Note*: estimates of growth in the number of internet users vary widely. The estimates quoted are conservative.

*Sources*: Internet Research Information Services, *IRIS Update*, 1997 (various issues), web site: http://iris.consultco.com:90/news.html, and Forrester Research, *The Forrester Report*, 1997 (various issues), web site: http://access.forrester.com/index.

204 Clearly, United States case law on electronic commerce is likely to reflect issues which will come before New Zealand courts in the future. United States case law on misuse of information through electronic means is of assistance in addressing whether there is a demonstrable need, in New Zealand, for better legal protection of information. We limit discussion to the practice of framing and the act of defaming. It is important to bear in mind that intellectual property rights already exist to protect information which is seen by the law as having proprietary characteristics. Thus, our assessment of the question posed in paragraph 202 is addressed in a wider context.

205 Framing is a variation of hyperlinking in which the linked site appears in an open window on the linking site.[312] The practice of framing involves two distinct issues: the confusion of consumers[313] and the commercial use (or misuse) of information. We concern

[312] ECom 1, paras 375–379.

[313] ECom 1, para 379.

ourselves here with the latter. It is important to remember that the linking of information of itself does not constitute misuse of information in any proprietary sense. In functional equivalent terms, one can say that framing a picture which has been purchased from an art gallery would not constitute misuse of the picture. But, when a hyperlink[314] in a website ("the hosting website") connects the user to another website ("the retrieved website") and presents the information in the frame of the hosting website then the information in the retrieved website may well appear to be an original product of the hosting website. The association created by the hyperlink may be positive or negative, depending upon a myriad of factors such as:

- the reputation of the hosting website;
- the influence the link will have on the number of "hits" to the retrieved website;
- whether the connection slows the speed of use of a website; and
- whether the connected website is a competitor of the retrieved website.

Assuming the retrieved website owner considers the association created is detrimental, does (or, should) that person[315] have any claim or action against the owner of the hosting website? And, if so, on what conceptual basis?

206 When framing is alleged to constitute misuse of commercial information, the common allegation in the United States is breach of copyright or trademark law. Inherently, such actions require a plaintiff to establish that the "information" is "intellectual property" to which rights at law exist. If the parties are contractually related the linking may amount to a breach of contract. There may also be a cause of action in trespass if the retrieved site has taken steps to notify users that linking is not permitted without consent, the forcefulness of which will be strengthened by the retrieved website having put in place technological barriers in an attempt to pre-empt linking.[316] Finally, in the United States there is a claim based on misappropriation.[317]

---

[314] ECom 1, paras 375–378.

[315] As opposed to a consumer who has been confused by the association.

[316] ECom 1, paras 147–157.

[317] See *NBA v Motorola Inc* 105 F3d 841 (2d Cir 1997) and M O'Rourke "Fencing Cyberspace: Drawing Borders in a Virtual World" (1998) 82(3) Minnesota Law Review 609, 697–701.

207 In New Zealand, four remedies that may be of assistance to a New Zealand litigant are (a) an action for breach of copyright,[318] (b) an action based upon section 9 of the Fair Trading Act 1986[319] (misleading or deceptive conduct in trade), (c) an action for unjust enrichment,[320] (d) a common law action for passing off[321] or (e) a claim based on unlawful interference with economic relations.[322] More generally, these causes of action, in addition to the actions discussed in ECom 1 (trespass to property, breach of confidence, negligence and defamation), provide protection against the misuse of information, whether that misuse causes loss to the person from whom it is obtained or confers a benefit (financial or otherwise) on the person who has acquired the information.

208 In determining whether there are any significant gaps in the law's protection of information an assessment is required of the protection afforded to information by existing causes of action. The difficulty of doing so is that most of the causes of action that may protect against the wrongful use of information are of common law or equitable origin. Common law and equitable causes of action have the characteristic of being evolutionary in nature, making them adaptable to new circumstances. Two maxims of equity demonstrate this inherent flexibility in relation to equitable causes of action:

- "Equity will not suffer a wrong to be without a remedy"; and
- "Equity looks on that as done which ought to be done".[323]

---

318 *Wellington Newspapers Limited v Dealers Guide Limited* [1984] 2 NZLR 66.

319 Burrows, Finn and Todd *Law of Contract in New Zealand* (8 ed, Butterworths, Wellington, 1997) 325–333.

320 Above n 319, 31 and 734 et seq and discussion of this tort at paras 221–227.

321 A Brown and A Grant *The Law of Intellectual Property in New Zealand* (Butterworths, Wellington, 1989) ch 3 and *Neumegen v Neumegen & Co* [1998] 3 NZLR 310.

322 S Todd (ed) *The Law of Torts in New Zealand* (2 ed, Wellington, Brooker's, 1997) ch 12 and subsequent discussion of this tort paras 217–220.

323 Butterworths New Zealand Law Dictionary (Butterworths, Wellington, 1995). See also ICF Spry *The Principles of Equitable Remedies: Specific Performance, Injunctions, Rectification and Equitable Damages* (5 ed, LBC Information Services, 1997).

209 Until particular cases involving the misuse of information come before our courts pleading reliance upon a common law or equitable cause of action, it is difficult to be emphatic that existing causes of action will provide a remedy. Our provisional view is that the protections offered by the action for breach of confidence (which is generally regarded as being of equitable origin), the tort of unlawful interference with economic relations and the claim of unjust enrichment (which is considered by some to be quasi-contract in nature and others as a restitutionary claim), as well as the wide ranging nature of section 9 of the Fair Trading Act 1986 (designed to provide a remedy for misleading or deceptive conduct in trade, or for conduct likely to mislead or deceive), should be sufficient to deal with most cases.

210 For convenience, we outline briefly the protections which are likely to flow from causes of action based on breach of confidence, unlawful interference with economic relations and the restitutionary claim based on unjust enrichment. We do not consider separately a cause of action based on section 9 of the Fair Trading Act 1986 as that is well known. The Court of Appeal has emphasised on a number of occasions that the words of section 9 of the Act should be given their ordinary meaning; the Court of Appeal has also emphasised the wide ranging nature of the remedial provisions contained in section 43(2) of the Act.[324]

### *Breach of confidence*

211 The law relating to breach of confidence has an inherent flexibility designed "to keep pace with changing social and economic circumstances and to cater for the needs and changing requirements of the times".[325]

212 Although information, of itself, is not regarded as property,[326] the breach of confidence action has been used to protect proprietary

---

[324] See *Goldsbro v Walker* [1993] 1 NZLR 394 (CA). Section 9 of the Fair Trading Act 1986 provides: "No person shall, in trade, engage in conduct that is misleading or deceptive or is likely to mislead or deceive".

[325] L Clarke *Confidentiality and the Law* (Lloyd's of London Press Ltd, London, 1990) xxii–xxiii.

[326] *Boardman v Phipps* [1967] 2 AC 46, (HL) 127 per Lord Upjohn.

interests in information.[327] However, authority is divided on whether such application is appropriate. At the very least it can be said that the breach of confidence action does have the potential to provide a remedy for the wrongful taking of information.[328] The case of *Franklin v Giddens* illustrates this potential. [329]

213 In *Franklin*, the plaintiff had, by a secret method of cross-breeding, produced a new type of tree. The defendant stole the specimens and thereby discovered the previously secret genetic structure of the wood. The plaintiff succeeded in an action for breach of confidence. Justice Dunn emphatically rejected the argument that there must be a private relationship of confidence between A and B before one could be liable to the other for breach of confidence. He was "quite unable to accept that a thief who steals a trade secret, with the intention of using it in commercial competition with its owner, to the detriment of the latter, and so uses it, is less unconscionable than a traitorous servant".[330]

214 The crux of the issue seems to be whether the circumstances are such that the person who acquired the information ought reasonably to know its confidential nature. Put more formally by Fullagar J in *Deta Nominees Pty Ltd v Viscount Plastics Pty Ltd*:[331]

---

[327] For example, in the Hong Kong case of *Linda Chih Ling Koo, John Ho Hung Chiu v Lam Tai Hing* CA Civ App No 116 of 1992, on appeal from HCA No A3466 of 1986, 14 April 1992, 23 IPR 607 (cited in E Loh, "Intellectual Property: Breach of Confidence?" (1995) 178 EIPR 405 at 405) Bokhary J stated: "A man's confidential information is his property. The courts have jurisdiction to protect such property from misuse. Such jurisdiction is not confined to cases in which such information has been imparted in confidence or to cases in which an obligation to keep the same confidential arises under contract. Any use, including self-use by the wrongdoer by force, menaces, trickery or stealth – is . . . misuse which is liable to be restrained or made the subject of an order for damages or an account". See also F Gurry, *Breach of Confidence* (Clarendon Press, Oxford, 1984) who views the existence of a proprietary right in confidential information as having only a very tenuous foothold; 406 in particular.

[328] This report does not purport to examine the merits of such development.

[329] [1978] Qd R 72 See ECom 1, para 163. See also the discussion of *Franklin* in Clarke, above n 325, ch 4 (Breach of Confidence and Privacy) and 5 (Information as Property).

[330] Above n 329, 80. See also *Boardman v Phipps* [1967] 2 AC 46; *Exchange Telegraph v Gregory* [1896] 1 QB 147; and *Francome v Mirror Group Newspapers Ltd* [1984] 2 All ER 408.

[331] [1979] VR 167, 193 cited in Clarke, above n 325, 106.

> Would a person of ordinary intelligence, in all the circumstances of the case, including, *inter alia*, the relationship of the parties and the nature of the information and the circumstances of its communication, recognise this information to be the property of the other person and not his own to do as he likes with.

215 Clarke is of the view that if it is a correct statement of the law to say that the person who obtained the information and others who have subsequently received it will be restrained from being able to use it then

> [t]here seems to be no reason why a hacker who dishonestly obtains unauthorised access to confidential information held on a computer should not be restrained from using that information by an action for breach of confidence.[332]

The main obstacle to such use of the action is a decision of Sir Robert Megarry VC in *Malone v Metropolitan Police Commissioner*.[333] In the Vice-Chancellor's view, "a person who utters confidential information must accept the risk of any unknown overhearing that is inherent in the circumstances of communication . . ."[334] – the means of communication in that case was by way of telephone.

216 Mindful of *Malone*, the Law Commission for England and Wales concluded that it was doubtful whether acquiring information by reprehensible means would render the obtainer of such information subject to an obligation of confidence.[335] The case could, of course, be easily distinguished on the effort required to "overhear" information conducted by electronic means as compared with telephonic means.

### *Unlawful interference with economic relations*

217 The leading case in New Zealand concerned with the tort of unlawful interference with economic relations is *Van Camp Chocolates Ltd v Aulsebrooks Ltd*.[336] *Van Camp* alleged that AB Consolidated Ltd (ABC) unlawfully interfered with its economic

---

[332] In Clarke, above n 325, 132.

[333] [1979] ch 344. See ECom 1, paras 165–166.

[334] Above n 333, 376.

[335] See ECom 1, para 162, where the words used in the Law Commission report (para 4.10) are quoted in full.

[336] [1984] 1 NZLR 354. A recent example of this tort being invoked is the case of *Dickson Livestock Associates Ltd v Wrightson Ltd* (28 April 1999) unreported, High Court Wellington, CP No 225/97; Goddard and Neazor JJ.

interests (the legal successor to the business and liabilities of ABC was Aulsebrooks). In summary, the basis of the allegation was that confidential information had been misused to produce a food bar of inferior quality which was associated by consumers with food bars manufactured by *Van Camp*. It was alleged that *Van Camp* had, in consequence, lost sales and that its trade reputation had been damaged. The Court of Appeal was asked to rule as to whether a claim based on a tort of unlawful interference existed.

218 Justice Cooke (as he then was), delivering the judgment of the Court, said: [337]

> As long ago as 1914 the tort was recognised in this Court in *Fairbairn, Wright & Co v Levin & Co Ltd* 34 NZLR 1 . . . Sim J delivering the judgment of Edwards J and himself said at pp 29–30 that '. . . if, for the purpose of advancing his own interests, a trader uses against a rival weapons that are unlawful and thereby causes him injury, the latter has a good cause of action for damages'.

After referring to *Merkur Island Shipping Corporation v Laughton*,[338] in which the House of Lords accepted that there is a tort of interfering with the trade or business of another person by doing unlawful acts, Cooke J concluded that the tort of unlawful inference is a recognised tort in New Zealand,[339] although:

> its boundaries will receive closer definition as cases emerge, and we see insufficient reason for discarding a judicial remedy which from time to time may be useful to prevent injustice.[340] . . . The essence of the tort is deliberate interference with the plaintiff's interests by unlawful means.[341]

219 It is unclear what kinds of acts may be relied upon to constitute the "unlawful means" requirement. The Court in *Van Camp* reserved its opinion on whether ". . . misuse of confidential information in breach of the defendant's duty to a party other than the plaintiff can constitute unlawful means for the purposes of this tort".[342]

220 The general nature of this tort does, in our view, provide a basis for the courts to develop principles dealing with misuse of business information in the electronic environment.

---

[337] [1984] 1 NZLR 354, 358–359.

[338] [1983] 2 All ER 189.

[339] [1984] 1 NZLR 354, 359.

[340] Above n 337, 359.

[341] Above n 337, 360.

[342] Above n 337, 360.

## *Unjust enrichment*

221 Burrows (et al) *Law of Contract in New Zealand* states:

> The law has for a long time had a series of rules enabling one person to recover money from another where the retention of money or some other benefit would unjustly enrich that other party at the expense of the first.[343]

We focus on receipt of a benefit.

222 The law of unjust enrichment will assist where "the plaintiff has conferred a benefit on the defendant in circumstances where it is fair that it should be paid for".[344] It is interesting to note that this area of law has changed from being referred to as "quasi-contract" to "restitution" because in reality most of the cases had "little or nothing to do with contract".[345]

223 With abandonment of the label quasi-contract, there has been a search for a principle to underpin this branch of the law. Although unjust enrichment of itself does not yet appear to be a sufficient basis for a cause of action, in New Zealand it has been referred to as an underlying rationale in claims of restitution. Put simply by Lord Browne-Wilkinson,

> . . . the concept of unjust enrichment lies at the heart of all the individual instances in which the law does give a right of recovery.[346]

224 While the limits of the unjust enrichment action are unclear, this means there is much room for development to ". . . mould the current complex mass of precedent into a new coherent whole".[347]

225 Professor Peter Birks has called for statutory clarification of the unjust enrichment action in terms of the following formula:[348]

---

[343] Burrows, Finn and Todd *Law of Contract in New Zealand* (8 ed, Butterworths, Wellington, 1997) 22.

[344] Above n 343.

[345] Above n 343, compare Burrows, Finn and Todd *Law of Contract in New Zealand* (8 ed, Butterworths, Wellington, 1992) chapter 21.

[346] *Woolwich Equitable Building Society v Inland Revenue Commissioners* [1993] AC 71, 197.

[347] Above n 343, 23.

[348] G Fitzgerald and L Gamertsfelder "Protecting Informational Products (Including Databases) Through Unjust Enrichment Law: An Australian Perspective" [1998] EIPR 244, 248.

(a) Unjust;

(b) Enrichment of the defendant;

(c) At the expense of the plaintiff;

(i) by subtraction from the plaintiff; or

(ii) by doing wrong to the plaintiff;

(d) Where no defences are applicable.

226 Fitzgerald and Gamertsfelder staunchly advocate that unjust enrichment law, more so than the traditional doctrines of tort, will emerge as the obligation which most adequately protects unjustified interference with information.[349] Without analysing the advantages and disadvantages of such development, the focus on the "benefit" in the cause of action lends itself to the contemplation of intangibles, which are the currency of the information industry. Another advantage of application of a restitutionary action to the misappropriation of information is the nature of the remedy; restitution is concerned with restoration to the plaintiff of the benefit received by the defendant, not with compensation for loss or damage.[350]

227 Fitzgerald and Gamertsfelder conclude:

> Unjust enrichment is to the information age what the tort of conversion was to the mechanical/industrial age. In essence they are the same obligation dealing with different degrees of tangibility. . . . Intellectual property lawyers should pay unjust enrichment more attention, as not everything will fall under the label of copyright or patent . . . and unjust enrichment lawyers should seek to exploit this golden opportunity to make their area of law the road map for the protection of intangible value in the information age.[351]

### *What is to be done?*

228 Issues involving electronic commerce are only just beginning to be litigated in New Zealand courts. The demand for added protection for information cannot be gauged until equity and the common law, in combination with statutory provisions such as the Fair Trading Act 1986, have been given the opportunity to meet such a demand. We are of the view that there is not, as yet, a

---

[349] See generally: Fitzgerald and Gamertsfelder, above n 348.

[350] Above n 348, 248.

[351] Above n 348, 255.

demonstrable need for legislative intervention to provide greater protection against the misuse of information.

229 We did not, in ECom 1, discuss these issues in as much depth. The further work which we have done meantime has led us to the view that there is a need to focus on whether existing statutory, common law and equitable actions are sufficient to meet the needs of those involved in electronic commerce. We invite submissions on this issue with the intention of addressing matters further in our third electronic commerce report which we intend to publish late 2000. In order to assist those who wish to make submissions on these issues we now put forward some ideas for future reform. We make it clear that these are no more than ideas and that, unless the contrary is expressly stated, the Commission has not yet formed views on their respective merits.

## IDEAS FOR FUTURE REFORM

230 As foreshadowed in our Computer Misuse report, we have considered the possibility of regarding information per se as *property*.[352] We have concluded that that course of action would be inappropriate for the following primary reasons:

- there would be considerable difficulty in determining what is property and what is not. There is no commonly accepted definition of "property". Problems also exist in attributing property rights to particular people.[353]
- in effect, the civil law would outstrip its criminal counterpart. Property per se is not protected under the criminal law. Society is protected against persons dealing with property in various ways, eg knowingly or recklessly or carelessly.
- as demonstrated by the above point, the effect of creating this new cause of action would be to cut across existing causes of action (notably intellectual property, passing off and breach of confidence), muddling existing law. The potential disturbance

---

[352] *Computer Misuse: NZLC R54* (Wellington, 1999) paras 21 and 36. See also RG Hammond "The Misappropriation of Commercial Information in the Computer Age" (1986) 64 Canadian Bar Review 342 where the difficulty of defining information as a property right is discussed.

[353] Assuming an adequate definition of "property" could be stated, there is the added difficulty of determining who created the property: how do you deal with numerous authors producing information?

of an "information as property" right to intellectual property law is illustrated by the following:

> The law has traditionally resisted characterising information per se as private property. As a matter of public policy the classical intellectual property system forbids the extension of exclusive statutory rights to products or processes that are not to some extent, inherently innovative. The regime is underpinned by the premise that intellectual property rights attach only to significant creative contributions that might not have been undertaken in the absence of reward or unfair competition. Copyright law gives creators limited property rights in their expression of ideas, but regards the information contained in a copyrighted work, like the work's ideas, to be in the public domain and available to be freely used by all.[354]

- a likely consequence of introducing a cause of action for wrongful "taking" of information will be that parties may no longer have adequate incentives to make their own provision for the importance of information to them.

## A NEW STATUTORY TORT?

231 Having rejected the redefinition of "information" as property, we considered other options for reform. We wish to raise, for submissions, whether it would be appropriate to consider enactment of a statutory tort 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. Legislation has just been introduced into Parliament to address certain aspects of computer misuse but it is far from clear whether that legislation will be passed in the form introduced or not.[355] Accordingly, we seek submissions on the question of whether users of electronic commerce believe there is sufficient uncertainty in the law to justify enactment of a statutory tort. If there is support for the concept we will examine it in detail in our third report.

232 At present, we tend to the view that if a statutory tort could be justified it should attract liability on proof, to the civil standard, that the criminal law had been breached. That would enable a party who has suffered loss, or can prove that the wrongdoer has obtained a profit, to recover that loss or an account of the profit

---

[354] G Evans and B Fitzgerald "Information Transactions Under UCC article 2B: The Ascendancy of Freedom of Contract in the Digital Millennium?" (1998) 21(2) UNSW Law Journal 404, 427 (footnotes omitted).

[355] See para 230.

from the wrongdoer on proof, on a balance of probabilities, that the wrongdoer has infringed the computer misuse legislation.

233 From a preliminary consideration of introducing a statutory equivalent to computer misuse, two factors will have significant influence on the desirability of introducing a civil equivalent to computer misuse:

- the interrelationship between the law of torts and the criminal law; and
- the availability of insurance to protect against the wrongful misuse of information.

We give a brief outline of these two issues for the assistance of those who intend to make submissions on these matters.

234 An alternative approach would be to consider the suggestion of Professor Birks[356] of codification of the law of unjust enrichment in the manner suggested by him. We invite submissions on whether that is an appropriate response to the issues raised.

### *The interrelationship between the law of torts and the criminal law*

235 The interrelationship between the law of torts and the criminal law raises the question whether it is appropriate for civil law remedies to be used, essentially by way of deterrence, in conjunction with criminal law measures enacted for that purpose. We say that because it is reasonably clear that many of those currently responsible for computer misuse will be of an age and of a means which will likely render civil liability empty. The difficult issues concerning the interaction of the civil and the criminal law was referred to, in passing, by Hammond J in *Powerbeat International Limited v Attorney-General*.[357] In the course of his judgment, Hammond J observed:

> . . . it has to be acknowledged that in many legal systems in the world today, the criminal law is given [primacy] even over the civil law in this area. For instance, in a notably high technology economy – that

---

[356] See para 225.

[357] (17 June 1999) unreported, High Court, Hamilton CP 72/98, 18–25. In *Powerbeat* Hammond J was faced with a set of facts which involved the execution of a search warrant against a premises owned by a company engaged in high technology processes. It was alleged that the search warrant was executed illegally or unreasonably and a cause of action was brought against the Attorney-General based on *Simpson v Attorney-General (Baigent's Case)* [1994] 3 NZLR 667 (CA).

of Japan – the primary line of attack on pirates and infringers is through the criminal law (see Doi, *Intellectual Property Protection and Management – Law and Practice in Japan* (1992)).

Whatever views may be taken on what are very difficult issues of public policy, and economics, there has in fact been increasing reliance on general criminal law provisions relating to dishonesty against pirates and copiers, with mixed success.[358]

The question inherent in Hammond J's observations is: should the criminal law alone deal with these types of issues?

### *The availability of insurance to protect against the wrongful misuse of information*

236 One of the purposes of the law of torts (in general) is to provide compensation for the wronged individual. However, as is stated by Balkin and David in *Law of Torts*,[359]

> If the principal aim of tort law is to provide compensation for many of the losses suffered through our modern way of life, that compensation will scarcely ever be effective unless the defendant is insured against his liability.

237 Mr C Nicoll[360] in *Insurance of E-Commerce Risks*[361] identifies three broad categories of e-commerce risks as being:

- *Business interruption*:
  A business may be brought to a standstill if its computer system ceases to work or its credibility is seriously compromised.
- *Legal liabilities*:
  The ability of a computer to present information to the outside world can bring legal liabilities down upon its proprietor and persons responsible for the information itself. The interactive nature of a computer can mean information in large volume may pass through or be stored within a system so its owner has no real editorial power over content. The interactive nature of a computer within a network also makes it a conduit for the

---

358 Above n 357, 23.

359 R Balkin and J Davis *Law of Torts* (Butterworths, Sydney, 1991) 7.

360 Christopher Nicoll, Senior Lecturer in Commercial Law, University of Auckland.

361 [1999] IJIL 293.

transfer of data in the form of an executable program. Such a program may cause damage to the system to which it is transferred. Specific risks of significance are: liability for the tort of defamation; liability for intellectual property infringement; liability for breach of confidential information; liability for negligent misrepresentation; liability under a contract made mistakenly by means of a computer; and liability for damage to a third party's system by the transfer to it of an executable program.

- *Penetration costs*:
  Security measures have become a challenge for the socially, although not technically, inadequate who will seek to penetrate systems not for financial gain but simply to leave a calling card or graffiti tag in the form of a virus (whether merely irritating or devastatingly destructive).

238 Based upon a consideration of the London insurance market, Nicoll concluded

> While cover of one sort or another seems to be available for most problems that can occur with e-commerce, "off the shelf" packages need careful consideration. The prudent proposer, at the present time, is advised to seek advice to ensure it gets a properly tailored product to suit its individual needs.

239 We seek submissions on whether the New Zealand insurance market provides adequate cover for e-commerce risks. We are particularly interested in establishing whether the cost of insurance cover is considered to be cost effective by businesses operating in electronic commerce. The adequacy or otherwise of an insurance market may have relevance to our consideration of whether a statutory tort is required.[362]

## LIABILITY OF INTERNET SERVICE PROVIDERS

240 The liability of an ISP – a secondary actor – is topical because it operates on a radically different basis to traditional carriers of communications. As put by Longdin:

> Technology allows operational malleability and providers can play more than one role or fit (or semi-fit) several functional metaphors from one moment in time to another. (. . . for example, a systems

[362] See ECom 1, para 178, and *South Pacific Manufacturing Co Ltd v New Zealand Security Consultants Limited and Henderson v Merretts Syndicates Limited* [1995] 2 AC 145.

operator could be functioning as a common carrier, broadcaster, or publisher simultaneously, or in quick succession, and a university could function as an Internet access provider as well as a cable service programme provider.)[363]

241 The liability of an ISP is also a matter of particular interest to plaintiffs in internet cases involving defamation as the ISP

- is more likely to have "deep pockets"; and
- is easier to locate than the primary publisher.

242 An ISP faces a diffuse range of potential liabilities. Liability could arise from such activities as: caching;[364] the uploading or downloading of information conducted by the ISP's subscribers; linking, framing, or hosting a website on which a defamatory message is published; and publishing.[365]

243 Service providers are categorised by Counts and Martin into three groups:

- the content provider;
- the pure access provider; and
- the mixed provider.[366]

The *content provider* would, for example, be the provider of a newspaper published on the internet. A *pure access provider* is a mere carrier, for example MCI Mail, which provides an electronic communication system through which subscribers communicate. In the United States, common carriers are exempt from liability resulting from the content of what they transmit provided certain

---

[363] L Longdin "Digital Transmissions and the Liability of On-Line Service Providers" (paper presented to the Fay, Richwhite Conference, Auckland, 15–16 July 1999) 13 (footnotes omitted). More generally, the discussion of ISPs' liability draws heavily on the content of the Longdin article.

[364] See the United States decision of *MAI Systems Corporation v Peak Computer Inc* 991 F2d 511 (9th Cir 1993) where it was held that caching amounted to reproduction of a copyrighted program. See also chapter 11, paras 178–179.

[365] Longdin, above n 363, 15–17.

[366] C Counts and A Martin "Libel in Cyberspace: A Framework for Addressing Liability and Jurisdictional Issues in this New Frontier" (1996) 59 Alb L Rev 1083. Other commentators prefer to divide travellers into groups that specify the nature of the use, for example, Longdin sets out the following ISP taxonomy for online intermediaries: common carriers or mere conduits; internet access providers; online hosts; information location tool providers and cyber-café proprietors (Longdin, above n 363, 12–15).

conditions are met.[367] The rationale for such an exemption is that it would be unfair to pin legal liability to common carriers when they are unable to alter harmful messages, unless given prior notice of their intended transmission.[368] Moreover, if common carriers were responsible for screening all of their messages, efficiency would be seriously impaired:

> Taken to its (il)logical extreme, such a rule could drive a phone company to prohibit real-time conversations between individuals, since the phone company would have to screen each sentence for potentially defamatory material.[369]

244 More difficult issues arise when the *content* and *pure access* functions are mixed. The internet content provider, in stark comparison, has control over the content of a publication and therefore can (rightly) expect to be held liable. Often the publisher edits every word prior to publication as well as selecting which material to publish and in what form.[370]

245 Both *content* and the *pure access* service providers have analogous counterparts in the real world. As a consequence, it should not be difficult to apply existing law to them. The same can not be said for a *mixed provider*.

246 A *mixed provider* necessarily fulfils roles of both *content* and *pure access* providers. There are not any industry standards for the role played by mixed providers; some exercise a great deal of editorial control over postings, while others merely provide the forum and abdicate responsibility for what is posted. Two United States actions against service providers illustrate how difficult it is to assess (and indeed predict) the legal responsibility of a mixed service provider.

247 In *Cubby Inc v CompuServe Inc*[371] the District Court found that a service provider that exercised no control whatsoever over the material accessed by its subscribers should be classified as a secondary publisher. The Court in *Cubby* stated:

---

[367] See Longdin, above n 363, 46 where the conditions are set out.

[368] P Niehaus "Cyberlibel: Workable Liability Standards?" [1996] U Chi Legal F 617, 619.

[369] Above n 368, 619–620.

[370] Above n 368, 621.

[371] 776 F Supp 135 (SDNY 1991).

> Compuserve has no more editorial control over such a publication than does a public library, book store, newsstall or news-stand, and it would be no more feasible for Compuserve to examine every publication it carries for potentially defamatory statements than it would be for any other distributor to do so.[372]

248 The inference arising from the *Cubby* case is that due to the size and speed of the internet an ISP is a mere distributor of defamatory material unless there is an aggravating factor. To require otherwise would be to require the ISP to monitor everything and thereby inhibit the flow of information.[373]

249 On the other hand, in *Stratton Oakmont Inc v Prodigy Services Co*,[374] the New York Supreme court held that a service provider which took steps to screen postings for offensive language and to enforce guidelines issued to its subscribers was exercising a degree of editorial control sufficient to make it liable as a primary publisher.[375] The trial court stated:

> Prodigy's conscious choice, to gain the benefits of editorial control, has opened it up to a greater liability than Compuserve and other computer networks that make no such choice . . .[376]

250 In our view, the "degree of editorial control" approach to determining the liability of a mixed service provider is undesirable for two reasons:

- first, it discourages screening for offensive material. Besides it being desirable for offensive material to be removed as frequently as possible, if ISPs are encouraged to *not* screen in order to avoid being considered a primary publisher, the effect

---

372 Above n 371, 140. ECom 1, paras 189–190. See also A Fitzgerald et al (eds) *Going Digital: Legal Issues for Electronic Commerce, Multimedia and the Internet* (Prospect Media, St Leonard, NSW, 1998) 156–157.

373 Above n 372, 157.

374 23 Media L Rep (BNA) 1794 (NY Sup Ct May 24, 1995). See ECom 1, para 189.

375 D Vick, L Macpherson and S Cooper "Universities, Defamation and the Internet" (1999) 62 The Modern Law Review 58, 64–65. Prodigy developed content guidelines and removed material that it believed would be harmful to the online community as well as using automatic pre-screening software and monitoring – in real time – the BBS using an emergency delete function to purge undesired messages: Counts and Martin, above n 366, 1097.

376 23 Media L Rep (BNA) 1794 at 1798 cited by Counts and Martin, above n 366, 1097.

would be to leave the defamed party with no legal redress at all, given the high likelihood that a judgment against an original publisher would be rendered empty because the original publisher was either unlocatable or impecunious.[377]

- secondly, the test is not sufficiently precise to provide an ISP with predictable criteria upon which to base their practices. The issue is: how much editorial control would be enough to trigger liability?[378] For example, does refusing to allow websites of a disreputable nature to link to your website constitute "editorial control".[379] An arguable analogy of this refusal in the real world is the editor of a magazine refusing to publish an article containing defamatory material.

251 It is not feasible nor fair to require ISPs to monitor content and remove material that is offensive or would give rise to a legal claim. Distributors do not have the resources or expertise to review all of the material they receive.[380] Even if they did:

- detection of legally actionable material will not often be caught by monitoring or packet sniffing technology.[381] For example, a word may not itself be defamatory but in its context may imply a defamatory meaning – subtle nuances can not be searched for through a conventional search engine;
- a search at 12 noon will not pick up a change (which may be minor but significant) at 12.05 pm – the ability to alter the information regularly is an important consideration;

---

377 See Niehaus, above n 368, 628.

378 Above n 368, 629.

379 The refusal may be either when there is a request to link prior to the act of linking, which is turned down, or a notification after linking that the link should be removed (and to fail to do so would then constitute a trespass).

380 See generally Niehaus, above n 368.

381 Longdin, above n 363 put it thus: "Certainly [monitoring or packet sniffing technology] may catch obscene or objectionable material by detecting the transmission of particular key words, terms or expressions but it is of dubious effectiveness in tracking defamatory statements or breaches of copyright or moral rights where much can depend on nuance and the juxtaposition of material". (18) "Packet sniffing" is "intercepting, analysing or recording communication packets (fixed size blocks of data which are transmitted over a communications channel) without altering the intercepted packets. The tools to accomplish this are freely available on the Internet": *NZLC R54* (Wellington, 1999) para 18.

- to hold ISPs liable may discourage the use of electronic commerce (and in particular the internet) by increasing the time and expense involved in digital transmission;[382]
- the speed of transmission and the large volume of digital traffic means that detection of infringement is likely to be (and can not, for the reasons that make content monitoring impracticable be anything but) after the fact.[383] And so, the issue becomes a factual one of how long should a legally objectionable message take to be removed by an ISP;
- requiring ISPs to remove, for example, a defamatory message, has the potential to impose on them a greater burden than their analogue counterpart: if a defamatory message is posted on a website and removed by the ISP that is not necessarily the end to the matter; there is nothing to prevent ongoing repostings (perhaps by a competitor), with the costs of locating and removing material falling on the ISP;[384] and
- monitoring itself could constitute a breach of privacy or, if our computer misuse legislation is enacted, unauthorised interception with data stored in a computer.[385]

252 It is however extremely important that mixed service providers can be certain of when their actions attract liability, and can encourage practices that remove and discourage the publication of illegal and offensive material on the internet. Hence we recommend liability be founded on actual knowledge. Counts and Martin have dubbed such a test "the graffiti principle",[386] using the case of *Heller v Bianco*[387] to illustrate that principle.

253 In *Heller v Bianco* a Californian appellate court found a tavern owner could be liable for a message scrawled on the bathroom that stated, in essence, "Call this number for a good time and ask for Isabelle". The tavern owner was informed of this message and asked to remove it by Isabelle's husband. The bar-tender responded that he would remove the message "when he got around to it", but failed to remove it. The court held that those "who invite the public" into their business have an obligation "not to knowingly" allow

---

[382] Longdin, above n 363, 17.

[383] Above n 363, 18.

[384] See Niehaus, above n 368, 624–625.

[385] Longdin, above n 363, 18.

[386] Counts and Martin, above n 366, 1099–1103.

[387] 244 P2d 757 (Cal Dist Ct App 1952).

their premises to be littered with "defamatory matter".[388] The court found:

> By knowingly permitting such matter to remain after reasonable opportunity to remove the same the owner of the wall or his lessee is guilty of republication of the libel . . . Republication occurs when the proprietor has knowledge of the defamatory matter and allows it to remain after a reasonable opportunity to remove it.[389]

We turn to look at how other countries are dealing with the liability of ISPs.

### *Overseas regulation of the liability of ISPs*

254 The Australian Bill does not include a provision dealing with the liability of ISPs.

255 The Singapore Government considers it essential to:

> . . . manage the exposure of network providers to risks of liability for third party content. The EC Policy Committee proposed that an ISP should not be held liable for third party content outside his control for which it merely provides access (for example, content of websites hosted overseas). However, the network providers will still be subjected to their obligations under existing licensing regimes from agencies . . . Network providers are also liable for their own content, or third party content which they adopt or approve of.[390]

256 The Singaporean Government's stance on ISP liability is reflected in section 10 of its Electronic Transactions Act 1998 which provides:

> **10 Liability of network service providers**
>
> (1) A network service provider shall not be subject to any civil or criminal liability under any rule of law in respect of third-party material in the form of electronic records to which he merely provides access if such liability is founded on –
>
> a. the making, publication, dissemination or distribution of such materials or any statement made in such material; or
>
> b. the infringement of any rights subsisting in or in relation to such material.
>
> (2) Nothing in this section shall affect –
>
> (a) any obligation founded on contract;
>
> (b) the obligation of a network service provider as such under a

---

[388] Above n 387, 758.

[389] Above n 387, 758.

[390] E-Commerce Business Policy "Main Guiding Principles" (unpublished, 1998) available at http://www.ec.gov.sg/ Sum3_08Apr98.html.

licensing or other regulatory regime established under any written law; or

(c) any obligation imposed under any written law or by a court to remove, block or deny access to any material.

(3) For the purposes of this section –

- "provides access", in relation to third-party material, means the provision of the necessary technical means by which third-party material may be accessed and includes the automatic and temporary storage of the third-party material for the purpose of providing access;
- "third-party", in relation to a network service provider, means a person over whom the provider has no effective control.

257 In Europe, there has been

> . . . considerable legal uncertainty within Member States regarding the application of their existing liability regimes to providers of Information Society Services when they act as "intermediaries", i.e. when they transmit or host third party information (information provided by the users of the service).[391]

The rationale for inclusion of provisions governing liability of intermediaries was to unify the stance to be taken by Member States as ". . . divergent principles have been adopted in those Member States which have introduced new legislation specifically addressing this issue".[392] The situation also leaves ". . . different parties (service providers, content providers, persons whose rights have been violated and consumers in general) under considerable legal uncertainty".[393]

258 Section 4 of the Proposal for a European Parliament and Council Directive on Certain Legal Aspects of Electronic Commerce in the Internal Market makes comprehensive provision for the liability of intermediaries. We reproduce section 4 (Liability of intermediaries) in full:

---

[391] Commission of the European Communities "Proposal for a European Parliament and Council Directive on Certain Legal Aspects of Electronic Commerce in the Internal Market" COM (1998) 586 final 98/0325 (COD) unpublished (Brussels, 18 November 1998) 12. Copy available from the Law Commission on request.

[392] Above n 391, 12.

[393] Above n 391, 12–13.

**Article 12**

**Mere conduit**

1. Where an Information Society service is provided that consists of the transmission in a communication network of information provided by the recipient of the service, or the provision of access to a communication network, Member States shall provide in their legislation that the provider of such a service shall not be liable, otherwise than under a prohibitory injunction, for the information transmitted, on condition that the provider:
   (a) does not initiate the transmission;
   (b) does not select the receiver of the transmission; and
   (c) does not select or modify the information contained in the transmission.
2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

**Article 13**

**Caching**

Where an Information Society service is provided that consists in the transmission in a communication network of information provided by a recipient of the service, Member States shall provide in their legislation that the provider shall not be liable, otherwise than under a prohibitory injunction, for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:

(a) the provider does not modify the information;
(b) the provider complies with conditions on access to the information;
(c) the provider complies with rules regarding the updating of the information, specified in a manner consistent with industrial standards;
(d) the provider does not interfere with the technology, consistent with industrial standards, used to obtain data on the use of the information; and
(e) the provider acts expeditiously to remove or to bar access to the information upon obtaining actual knowledge of one of the following:
   – the information at the initial source of the transmission has been removed from the network;

– access to it has been barred;
– a competent authority has ordered such removal or barring.

**Article 14**

**Hosting**

1. Where an Information Society service is provided that consists in the storage of information provided by a recipient of the service, Member States shall provide in their legislation that the provider shall not be liable, otherwise than under a prohibitory injunction, for the information stored at the request of a recipient of the service, on condition that:
   (a) the provider does not have actual knowledge that the activity is illegal and, as regards claims for damages, is not aware of facts or circumstances from which illegal activity is apparent; or
   (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.
2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

**Article 15**

**No Obligation to Monitor**

3. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.
4. Paragraph 1 shall not affect any targeted, temporary surveillance activities required by national judicial authorities in accordance with national legislation to safeguard national security, defence, public security and for the prevention, investigation, detection and prosecution of criminal offences.

259 There seems to be a number of consistent themes running through the way in which various States are dealing with this issue. For example,

- In California, the touchstone is actual knowledge of the existence of objectionable or defamatory information and a failure to remove the information in a timely fashion.[394]
- In Singapore, an ISP is not liable to criminal or civil sanctions provided its role is merely to provide access. The term "third party" is defined in section 10(3) of the Electronic Transactions Act 1988 (Singapore) to mean a person over whom the ISP has no effective control; presumably control (and, hence, an ability

[394] See paras 252–253.

to control publication) would exist at the time that actual knowledge of the existence of objectionable or defamatory material is obtained.

- The touchstone for no liability under the proposed European Union Directive is that the ISP is a mere conduit, or received information by way of caching of which it has no knowledge, or has no actual knowledge that an activity is illegal or knowledge of facts or circumstances from which illegal activity is apparent. Once actual knowledge exists, there is an obligation to act expeditiously to remove or to disable access.

260 In our view, legislation should clarify that ISPs have no liability unless they have *actual knowledge* of the existence of information on the website which would be actionable at civil law or constitute a crime. The legislation should go further to provide an obligation to remove promptly any information drawn to an ISP's attention. But it should also be made clear that the ISP is not liable for any reposting of that information by a third party unless or until it obtains actual knowledge of reposting and fails to act to remove. We recommend accordingly.

261 This recommendation is of a general nature. It is intended to clarify the circumstances in which an ISP may be liable. We contrast this recommendation with our specific recommendation in relation to the Defamation Act 1992 which, because of its nature as a statutory defence, requires a specific provision rather than a general one.[395] This recommendation is intended to cover all actions (other than those of contractual origin in which the contract defines the obligations) brought against ISPs. Examples of cases to which the provision would apply are actions under section 9 of the Fair Trading Act 1986 and tortious claims.

### *Defamation*

262 Defamation is one example of a tortious action. The potential effect of defamation law on discourse over the internet

> . . . has attracted considerable comment, in part because a high proportion of the small number of [overseas] lawsuits arising out of Internet communications have involved defamation claims . . . Actions have been brought in Australia, the United Kingdom, and the United States.[396]

---

[395] See para 269.

[396] Vick, Macpherson and Cooper, above n 375, 58 and footnote 2.

The potential for defamation of third parties is an important issue in the context of an electronic medium which provides an ability to publish a statement both widely and anonymously.

263 In ECom 1, after considering overseas case law, we stated:

> There is little doubt that electronic transmission of a defamatory statement which identifies the plaintiff constitutes publication for which the publisher will be liable . . . The main issue is not therefore *whether* liability in defamation can arise from electronic communications, but rather *who* may be liable and, in particular, whether network service providers may be liable for publishing defamatory comments made by their subscribers.[397]

264 We then examined the potential liability of ISPs and concluded that liability would turn upon a factual conclusion as to how much editorial control the ISP had over the defamatory material. As to the availability of the defence of innocent dissemination provided for by section 21 of the Defamation Act 1992 (set out at ECom 1, para 190),[398] we expressed the view that that:

> The definitions of "processor" and "distributor" in section 2(1) of the Defamation Act 1992 are probably sufficiently broad to include computer network service providers.[399]

Section 2(1) of the Defamation Act 1992 defines a "Distributor" as including a bookseller and a librarian; and a "Processor" as meaning ". . . a person who prints or reproduces, or plays a role in printing or reproducing, any matter".

265 Since publication of ECom 1, Morland J in *Godfrey v Demon Internet Ltd* (*Demon*)[400] has considered the ability of an ISP to avail itself of the defence of innocent dissemination provided for by the United Kingdom Defamation Act 1996, section 1.[401] The relevant part of section 1 of the Defamation Act 1996 (UK) provides:

> (1) In defamation proceedings a person has a defence if he shows that –
> (a) he was not the author, editor or publisher of the statement complained of,
> (b) he took reasonable care in relation to its publication, and

---

397 ECom 1, para 187.

398 At common law, the innocent dissemination defence was developed because it was perceived to be unreasonable to expect libraries, newsagents, and booksellers to screen the contents of every publication they distributed.

399 ECom 1, n 74.

400 [1999] 4 All ER 342.

(c) he did not know, and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement.

(2) For this purpose . . . "publisher" means a commercial publisher, that is, a person whose business is issuing material to the public, or a section of the public, who issues material containing the statement in the course of that business. . . .

266 The distinction drawn in the New Zealand and United Kingdom legislation is between primary and secondary publishers. The importance of the distinction is that only a secondary publisher can invoke the defence of innocent dissemination.

> The [United Kingdom] Defamation Act 1996 sends mixed signals to service providers regarding their responsibility for what is posted and accessed through their computer systems. On the one hand, any steps taken to exercise a measure of control over the content of Internet communications might be interpreted as inconsistent with being "only involved" as a provider of access to the Internet, as evidence that computer users are not beyond the "effective control" of service providers, or even that service providers exercise editorial control over the messages posted by their users. On the other hand, a *laissez faire* approach could be interpreted as a lack of reasonable care, particularly when alternatives are available that conceivably could reduce, or limit access to, abusive messages on the Internet.[402]

267 In *Godfrey v Demon Internet Ltd*, the judge found that the ISP was not a "publisher" for the purposes of section 1(2) of the United Kingdom statute; accordingly, subsection (a) of the section 1(1) defence was satisfied as *Demon* was not an author, editor or publisher of the statement complained of. But, the judge struck out the defence because *Demon* had been asked to remove the offending material and had failed to do so and therefore it could not meet the requirements of section 1(c) of the (UK) Defamation Act 1996.

268 Technological responses will block access to websites with obvious examples of defamatory statements (ie obscene, indecent, abusive or racist content). Software currently used for such purpose include Cyber Patrol, CYBERsitter, Net Nanny and Surfwatch. It is not

---

[401] Section 1 of the Defamation Act 1996 (UK) has been described as a "modern equivalent of the common law defence of innocent dissemination": per Lord Mackay LC Hansard, 2 April 1996, Col 214 Defamation Bill (HL) cited in *Godfrey v Demon Internet Ltd*, above n 400.

[402] Vick, Macpherson and Cooper, above n 375, 77

however feasible, nor desirable, to carry out extensive blocking or monitoring (refer to para 250). Indeed, an ISP could be courting liability if it exercises control over the material accessed by its subscribers. The case of *Stratton* illustrates that point.[403]

269 In our view, there is a need for ISPs to be protected through the innocent dissemination defence provided by section 21 of the Defamation Act 1992. While, in ECom 1,[404] we indicated that an ISP would probably fall within the definition of "processor" and "distributor", on reflection we tend to the view that the law should be amended to remove any residual doubt. It is not inconceivable that a judge, interpreting those definitions, could come to the view that they did not include an ISP. Accordingly, we recommend that the problem be solved by including in the definition of "distributor" reference to an ISP. Internet Service Providers should then be defined in a separate definition to include providers of the services discussed in para 242.

270 This would be consistent with the approach which we have recommended in relation to ISP liability generally. We recommend an amendment to the Defamation Act 1992 accordingly.

---

[403] See para 249.

[404] See ECom 1, n 74.

# 14
# Conflict of laws

271 CONFLICT OF LAWS (or private international law) is the body of law concerned with the special issues that arise where dealings between parties, or disputes, have connections with more than one country. New Zealand conflict of laws rules address the four broad issues that arise where a dispute involves a foreign element:[405]

- whether the New Zealand court can exercise jurisdiction to hear the dispute;
- whether the New Zealand court will exercise jurisdiction, or will decline to do so and leave the dispute to be resolved in the courts of another country;
- by reference to which country's laws the various issues in the dispute will be resolved – this is referred to as the question of "choice of law"; and
- whether a foreign judgment will be enforced in New Zealand, or recognised by the New Zealand courts as determinative of a dispute or of some issues in a dispute.

272 As explained in ECom 1, each country has its own conflict of laws rules. There are significant differences between New Zealand's conflict of laws rules and those of many other countries. Difficult practical problems arise where differences in conflict of laws rules result in inconsistent answers being given to the issues identified above. Indeed, even where countries have identical conflict of laws rules, the way in which those rules are framed can result in unsatisfactory outcomes such as a judgment given in the country with the closest connection with the dispute not being recognised and enforced in the other.[406]

273 The increasing importance of electronic commerce requires a renewed focus on conflict of laws rules:

---

[405] ECom 1, para 254.

[406] For a discussion of the unsatisfactory state of New Zealand's conflict of laws rules, and the need for multilateral reform, see D Goddard "Global Disputes – jurisdiction, interim relief and enforcement of judgments" (paper presented to New Zealand Law Conference, Rotorua, April 1999).

- where a person or company makes material available on a website, that material can be accessed and read by millions of people in many different countries. This immediately raises questions of the application of foreign laws to the content of the site, and to dealings resulting from it;
- the increased ease of dealing across borders has resulted in a huge increase in the number of interactions and disputes which, because they are not purely domestic, raise conflict of laws issues;
- the parties to many of these cross-border dealings are not experts in cross-border trade, and many of the transactions involve relatively small amounts of money. So it is less likely that they will have addressed conflict of laws issues in their dealings in advance, for example by expressly agreeing where disputes will be resolved, or which law or laws will govern their dealings;
- many current rules in relation to jurisdiction, and to a lesser extent choice of law, turn on where a certain person was at the time of the relevant event, or where some act took place (eg a publication of defamatory material, or entry into a contract, or performance of that contract). Applying these tests is much more difficult – perhaps impossible – where the parties deal online. Even where these tests can be applied, the answer is often quite fortuitous, with no substantive connection to the relevant dealings or dispute.

274 There is also the difficulty of internet communication having numerous participants, as illustrated by Longworth's commentary:

> Given the transnational nature of the communications, it will prove exceedingly difficult to determine which jurisdiction should apply. For example, in any interaction in cyberspace there is an uploader (of information), a downloader, the potential to access or view information, a server containing the web page files, the routing of data in packets through nodes around the world, the practice of constituent parts of a web page (such as images) being called up from other servers, links from the web page to other pages from elsewhere in cyberspace, and the intervention of sysops. Each of these actors and activities may be 'located' in different jurisdictions. It will be the norm rather than the exception that these participants are unknown to each other (rather than being seen as senders and recipients in a pre-determined relationship).[407]

---

[407] E Longworth *Possibilities of a Legal Framework for Cyberspace – Including a New Zealand Perspective* (GP Publications, Wellington, 1999) 35 citing D Menthe "Jurisdiction in Cyberspace: A Theory of International Spaces" (1998) 4 Mich Tel Tech L Rev 3.

275 The challenges which electronic commerce poses for the conflict of laws fall into two quite distinct categories. First, there are issues which are peculiar to the electronic environment, such as the difficulty of applying some traditional tests in that environment, and the unpredictability of the outcome of applying such tests. The second, more general category of issue is not in fact peculiar to electronic commerce – rather, all that electronic commerce is doing is increasing the frequency with which more general problems arise in cross-border disputes, highlighting existing deficiencies in private international law regimes.

276 With a view to addressing the special issues that arise where parties deal electronically, at least in the short term, and in particular to enhance the predictability of the application of existing New Zealand conflict of laws rules to e-commerce, ECom 1 proposed introduction of the following presumptive rules:[408]

- in an international contract for the sale of goods,
  - the courts of the State to which the goods are to be delivered *prima facie* be considered *forum conveniens*.
  - the contract will be governed, . . . by the law of the state to which the goods are delivered.
- in an international contract for the provision of services,
  - the place at which the services are to be performed will be the forum in which any dispute arising is to be resolved.
  - the place at which the services are to be performed will determine the law under which the dispute shall be resolved.

The longer term initiative we proposed was to ". . . encourage international discussion with a view to formulating a convention likely to be acceded to by most of New Zealand's major trading partners".[409]

277 The few submissions received in response to these proposals are set out below:

> The presumptive rule as to choice of laws, is very attractive. It would provide certainty, as suggested, especially in relation to consumer contracts. In this respect it would also be consistent with the direction of the OECD Guidelines. However, as a short term, and essentially unilateral measure, there seems little point in passing legislation.[410]

---

408 ECom 1, paras 289 and 296.

409 ECom 1, paras 290 and 297.

410 Joint submission of the Ministry of Commerce and the Ministry of Consumer Affairs, para 13.

> The Commission suggests . . . presumptive rules for choice of forum, and . . . for choice of law. . . . The Committee supports these proposals as interim measures until a more comprehensive solution is available by international convention.[411]
>
> With regard to international reforms, the advent of electronic commerce will ultimately increase the level of integration between the New Zealand and global economies. Telecom would therefore encourage the Law Commission to take an active role in appropriate international fora in order to present a New Zealand perspective.[412]
>
> The proposal to introduce presumptive choice-of-law rules for contract disputes may be supported in principle, but the specific rules proposed are crude; . . . The proposal to amend the New Zealand law on jurisdiction and recognition of foreign judgments is ill-timed, as work will soon commence at the Hague on an international convention on these matters and it would be inappropriate to engage in idiosyncratic legislative reform at this juncture.[413]

278 Having considered these submissions, and discussed them with the Advisory Committee, the Commission has decided not to recommend short-term legislative solutions along the lines canvassed in ECom 1.

279 Instead, the Commission has focused on the longer-term objective of multilateral coordination, and has been able to coordinate representation of New Zealand at the Hague Conference discussions in relation to a proposed convention on jurisdiction and enforcement of judgments in civil and commercial matters.[414]

---

[411] Submission of the Commercial and Business Law Committee of the New Zealand Law Society, 5.

[412] Submission of Telecom New Zealand Ltd, para 8.

[413] Submission of Mark Perry and Laurette Barnard, 3.

[414] The Hague Conference on private international law is an intergovernmental organisation the purpose of which is "to work for the progressive unification of the rules of private international law" (Statute, article 1). The principal method used to achieve the purpose of the Conference is the negotiation and drafting of multilateral treaties or conventions in the different fields of private international law (international judicial and administrative cooperation; conflict of laws for contracts, torts, maintenance obligations, status and protection of children, relations between spouses, wills and estates or trusts; recognition of companies; jurisdiction and enforcement of foreign judgments). After preparatory research has been done by the Secretariat (the Permanent Bureau of the Hague Conference), preliminary drafts of the conventions are drawn up by the Special Commissions made up of governmental experts. The drafts are then discussed and adopted at a Plenary Session of the Hague Conference, which is a diplomatic conference. For further information in relation to the Hague Conference, and its current work, see its website at http://www.hcch.net.

In particular, the Commission has encouraged the Hague Conference to pay close attention to electronic commerce issues in formulating the proposed convention. While the convention is primarily directed at resolving deficiencies of a general kind in private international law regimes, it is essential that it does so in a way which also addresses problems of the second kind identified above, and establishes rules which can be readily and predictably applied where parties deal electronically.

280 The biggest drawback of international treaties is of course their painstakingly slow creation.[415] But despite this, there are compelling practical reasons for participating in the work of the Hague Conference in this field:

- the nature of these problems – in particular, the lack of consistency and coordination in how different countries respond to the four issues identified in paragraph 271 above – means that they can only be resolved multilaterally, through an initiative involving a large number of countries;
- the Hague Conference is a body with substantial expertise and experience in private international law treaty-making. The Conference's 46 member countries include all New Zealand's major trading partners.[416] New Zealand, though not a member of the Hague Conference, is a party to two of the treaties formulated by the conference in this field;
- work on the proposed convention is well advanced. At the June 1999 meeting of the Hague Conference the text for roughly two-thirds of a draft convention was discussed and provisionally approved. The balance of the draft will be discussed at a one week meeting in October 1999, and the entire text will be reviewed and approved for submission to a Diplomatic Conference scheduled for October 2000. The Diplomatic Conference, which is the decision-making body of the Conference, is expected to approve a final text of the convention at the session in October 2000, and the convention would then be opened for ratification by Member States and other States such as New Zealand.

---

[415] Longworth, above n 407, 36.

[416] The current members of the Hague Conference on Private International Law are: Argentina; Australia; Austria; Belgium; Canada; Chile; China; Croatia; Cyprus; Czech Republic; Denmark; Egypt; Estonia; Finland; Former Yugoslav Republic of Macedonia; France; Germany; Greece; Hungary; Ireland; Israel; Italy; Japan; Republic of Korea; Latvia; Luxembourg; Malta; Mexico; Monaco; Morocco; Netherlands; Norway; Poland; Portugal; Romania; Slovakia; Slovenia; Spain; Suriname; Sweden; Switzerland; Turkey; United Kingdom; United States of America; Uruguay; Venezuela.

281 As a result of his involvement in the work of the Hague Conference session in June 1999, Mr David Goddard, New Zealand's representative at that session, was asked to attend a three day "Round Table" in Geneva in early September 1999 to discuss the challenges electronic commerce poses for private international law. The meeting was jointly organised by the Hague Conference and the University of Geneva, and focused on the extent to which the current draft of the proposed Hague Convention adequately accommodates electronic commerce issues, as well as considering whether further multilateral initiatives are required in the field of private international law, for example to address questions of choice of law. The conclusions of that Round Table will assist the Hague Conference to develop a convention which is suitable for an environment where a significant (and increasing) proportion of cross-border dealings will take place electronically. Mr Goddard also attended the meeting of the Hague Conference on private international law in October 1999.

282 In the circumstances, it would be premature to embark on a detailed consideration of conflict of laws issues in this report. Once the draft convention has been finalised later this year, however, it will be timely to consider both the content of that draft, and whether New Zealand should seek to become a member of the Hague Conference prior to the October 2000 Diplomatic Conference which will discuss (and is expected to adopt) a convention on these important issues. We will address these topics in our third report.[417]

283 We make one final point: it is clearly preferable to harmonise laws to avoid or to reduce the possibility of conflict of laws issues arising. The recommendations made in this report are largely supportive of the Australian Bill. We urge Parliamentary Counsel to consider drafting our proposed Electronic Transactions Act in a manner consistent with the Australian Bill so as to minimise the potential for conflict of laws issues to arise.

---

[417] See para E5.

# 15
# Banking

284 In ECOM 1 we raised a number of issues regarding the issue of "electronic money" (EM) and many submissions were received on this point. They were almost unanimous in concluding that at present it seems unnecessary to require issuers of EM to register as banks under the Reserve Bank of New Zealand Act 1989, unless they purport to carry out other banking activities. This is because:

- registration would not solve difficulties in regulating EM issued offshore;
- the rapid rate of technological development is not compatible with specific controls;
- it could create double regulation, eg in relation to credit card payments;
- the issue of EM is already covered by the Securities Act 1978;
- it would conflict with the non-discrimination principle, and may inhibit businesses from issuing EM;
- EM is unlikely to have a large impact as consumers will be subject to small limits and the existing framework can accommodate it. This is because New Zealanders (unlike overseas consumers) tend to use EFTPOS (Electronic Funds Transfer at Point of Sale) even for very small transactions, so EM will have to compete in a market that is already well serviced.

285 No submissions were received commenting on whether further steps, beyond redefining "writing" and "signature" to include electronic equivalents, were required to facilitate electronic banking transactions.[418]

286 Furthermore the submissions indicate that it is not necessary to introduce specific legislation to deal with laundering of EM or

[418] Refer to discussion in chapter 2, The Need for Legislation, paras 28 and 30 regarding the definitions of "writing" and "signature" respectively.

defaulting issuers as it is not possible to predict how these will be conducted; ie by what means.[419]

287 EM has the potential to facilitate money laundering as it is less conspicuous than large amounts of cash, and can be transferred around the world instantly. It is also anonymous, as it can be transferred without any physical encounter. However there are some aspects of EM which can aid in the detection and suppression of illegal activity. Systems can generate a detailed audit trail. Limits can be placed on the amount of EM carried on smart cards, and on the number of face-to-face transactions that can be made before the EM has to be encashed through an intermediary financial institution. At that point, the reporting requirements for financial institutions are activated.

288 The Financial Transactions Reporting Act 1996 (FTRA) aims to prevent and detect money laundering by imposing obligations on financial institutions to verify the identity of persons conducting transactions (sections 6–7), to report suspicious transactions (section 15) and to keep transactions records (section 29). It is however, arguable whether issuers of EM would be considered to be "financial institutions" under the FTRA. The definition in section 2 is wide and includes banks registered under the Reserve Bank of New Zealand Act, as well as

> (k) Any person whose business or a principal part of whose business consists of any of the following: . . .
>
> (v) Providing financial services that involve *the transfer or exchange of funds, including (without limitation) payment services*, foreign exchange services, or risk management services (such as the provision of forward foreign exchange contracts); . . .". (emphasis added)

Arguably the issue of EM constitutes "transfer or exchange of funds". However if issuers of EM were required to comply with the FTRA they would incur compliance costs which could in turn hinder competition.

289 The submissions concluded that no amendments to legislation were currently required. It was, however, suggested that the Reserve Bank should undertake review of the FTRA in the near future to ensure fraudulent and other illegal activities involving EM are within the scope of the FTRA. We leave that issue to the Reserve Bank to consider further.

---

[419] This view is supported in S Welling and A Rickman "Cyberlaundering: The Risks, The Responses" (1998) 50(2) Fla L Rev 295.

## The movement of money across borders

290 Since the abolition of exchange controls, the movement of money internationally has ceased to be an issue, according to submissions made by the Reserve Bank. Under section 37 of the FTRA everyone arriving or leaving New Zealand with cash of or in excess of NZ$10 000 must make a report to the Customs Service. "Cash" is defined in section 2 as "any coin or paper money that is designated as legal tender in the country of issue". This definition would not appear to encompass EM.

291 No immediate problems arise in allowing EM issued in one country to be redeemed in another, as only the issuer can "redeem" the value issued, so cross-border issues will not usually arise. The spending of EM in another country can be equated with the spending of travellers cheques.

292 A possible obstacle to conducting transactions over the internet is where the merchant is obliged to bill overseas purchasers in New Zealand dollars.[420] While many websites incorporate a currency converter so the purchaser can calculate the approximate price in his or her own currency, the end price will still fluctuate with the exchange rate. This uncertainty can operate as a barrier to commerce as consumers prefer to know exactly how much they will be charged, in their own currency, before making the decision to purchase. However, New Zealand banks currently only accept credit card vouchers denominated in domestic currency, although the possibility of enabling foreign currency transactions is being investigated.[421]

293 A local private sector initiative is tackling this obstacle, offering a service in conjunction with a British bank which enables retailers to bill customers in up to six different currencies. Merchants must satisfy credit checks before availing themselves of the service, which can be problematic for new companies without a credit history.[422] A possible solution the company is considering is to impose an upper purchase limit on transactions undertaken by these merchants.

---

[420] This problem was cited as a reason for establishing a "National Office on the Information Economy" in *The Independent*, 7 July 1999, 23.

[421] See "Multiple Currencies for Exporters" *NZ Infotech Weekly*, *The Dominion*, 26 April 1999, 1.

[422] See "Young NZ Retailers blocked from Net Payment Service" *NZ Infotech Weekly*, *The Dominion*, 2 August 1999, 3.

## LIABILITY FOR UNAUTHORISED ELECTRONIC TRANSACTIONS

294 An issue which we did not address in ECom 1 was the question of who should bear the risk of unauthorised electronic banking transactions. This is an issue which we now explore. We have explained in broad terms the competing viewpoints. We request submissions on the issues raised so that we can address them further in our third report.

295 Electronic transactions have become increasing popular in the banking environment over the last 20 years.[423] In the retail sector these transactions take place through automatic teller machines and EFTPOS terminals. In addition, consumers can use telephone and internet banking services, and the use of stored value cards and digital cash seems likely to develop (although at the time of writing no New Zealand bank had yet issued any). [424]

296 These electronic systems require some form of electronic authentication, such as a password or a code like a four digit PIN. The use of these forms of authentication can make it difficult to detect an unauthorised transaction as, unlike a manual signature, a password or pin is identical whether used by an authorised user or not. The issue then arises as to what extent the payment system provider or its customers should be liable for unauthorised use. In the manual world, the bank normally bears the risk for forgery.[425]

297 By way of analogy, we refer to the case of unauthorised credit card transactions. When an unauthorised credit card transaction occurs, a "charge-back" can be effected so that the customer is reimbursed the disputed amount and the merchant is debited. If the merchant is unable to pay then the bank carries the loss rather than the consumer. The rationale for offering such a high level of protection to the consumer is to encourage use of the credit card facility.[426]

298 All that is required to effect a charge-back is that the consumer makes a request to the bank in writing. The mechanism is not

---

[423] New Zealand leads the world in EFTPOS penetration, with one terminal per 63 people. In 1993 cheques constituted 54 percent of all transactions, by 1997 this had fallen to 27 percent in favour of electronic transactions (*New Zealand Official Yearbook 1998*, 559).

[424] ECom 1, paras 354–360.

[425] Section 24(1) of the Bills of Exchange Act 1908. In relation to collecting banks see section 5 of the Cheques Act 1960.

[426] This contrasts starkly with the banks' approach to customer liability in respect of transactions effected using PIN numbers, discussed in paras 305–312.

restricted to cases of fraud but can also be used where a merchant has failed to deliver goods, for example. In general the bank is under no obligation to verify the consumer's claim or carry out any checks on the card when a request is made; if the merchant considers that the claim is not bona fide then its only option is to initiate proceedings against the consumer.

299 Brownsword and Howells[427] identify four potential avenues in contract law for challenging a clearly drafted charge-back clause:

- the clause has not been incorporated, ie that "reasonable notice" of the clause has not been given: *Thornton v Shoe Lane Parking Ltd*.[428] A merchant would be unlikely to succeed on this basis unless shortcuts were taken in presenting the clause;
- the clause does not apply to the facts because if it were it would produce an unreasonable outcome. If on an ordinary construction the clause produces an unreasonable result then the court may be prepared to consider a less obvious construction: *Lancashire County Council v Municipal Mutual Insurance Ltd*.[429]
- the clause contravenes the Unfair Contract Terms Act 1977 (UK);[430]
- to enforce the clause would violate principles of good faith and unconscionability. However these doctrines are used sparingly and would be unlikely to be applied in relation to a feature of everyday dealing such as a charge-back clause.

300 Brownsword and Howells conclude[431] that it is unsatisfactory for retailers to have to rely on "occasional judicial interventions" in their favour in cases of credit card fraud by someone other than the cardholder. They recommend that credit based dealings be regulated in such a way that the interests of all participants are fairly represented.

301 The Banking Ombudsman has also expressed concern at the number of complaints received regarding credit card transactions made by telephone/mail order and the authority given by the actual

---

427 R Brownsword and G Howells "When Surfers Start to Shop: Internet Commerce and Contract Law" (1999) 19 Legal Studies 287–315.

428 [1971] 2 QB 163

429 [1996] 3 All ER 545

430 This United Kingdom statute renders certain types of clauses totally ineffective and subjects others to a test of reasonableness. There is no exact legislative equivalent in New Zealand.

431 Above n 427.

credit card owner.[432] These complaints generally submitted that when a merchant rang a credit card company for authorisation of a transaction, it was under the impression that authorisation meant the payment was guaranteed. The Banking Ombudsman did not uphold any of these complaints as it was found that the transactions were governed by the merchant's contract with the banks, which stated (although perhaps not as clearly as it ought) that referral for an authorisation number did not constitute a guarantee. The Banking Ombudsman noted that the limited guidance to merchants seemed to be prefaced on the assumption that most credit card transactions took place face-to-face, and that it was out of date.[433]

302 Some of these issues fell to be considered by the High Court in the recent decision of Master Thomson in *The Laptop Co Ltd v ANZ Banking Group* (New Zealand) Ltd.[434] In that case the plaintiff company took 34 telephone orders from a person in the United Kingdom for computer hardware. Payment was to be made with 18 personal credit cards . For each transaction the plaintiff obtained authorisation from its bank, the defendant. The telephone orders were in fact fraudulent. The defendant bank told the plaintiff it would not honour the authorised transactions, and debited the amounts it had previously credited to the plaintiff's bank account. The plaintiff was able to halt some deliveries of the hardware but sued for the shortfall, claiming breach of contract, and misleading or deceptive conduct under the Fair Trading Act 1986. It was held that there had been no breach of contract by the bank. A clear construction of the standard form agreement and operating guide showed that obtaining authorisation from the bank was no guarantee of payment.[435]

303 In the short term, banks who offer credit card transaction processing services to merchants should educate their merchant customers of the risk that payment for "remote" orders (via telephone/fax/internet) will be charged back to them if the transaction is not authorised by the cardholder, and that authorisation does not constitute guarantee of payment.

---

[432] Annual Report 1997/1998 Office of the Banking Ombudsman 22–23.

[433] Above n 423, 36–37.

[434] (1999) 6 NZBLC 102, 833, 99–474.

[435] See n 434, 102, 842. The proceeding in respect of the Fair Trading Act 1986 action was transferred to the District Court, as the Master dismissed the defendant bank's application for summary judgment against the plaintiff in respect of this cause of action. The case is yet to be heard in the District Court (102, 843).

304 On the other hand, it must be noted that a bank or a credit card company has no control over the way in which its products are used by the customer. The customer may fail to take care of his or her card or may not advise the bank or credit card company in a timely fashion if the device is compromised.[436] Where control of the credit or debit card primarily rests on the consumer, it is not surprising that banks seek to allocate risk in their favour. An allocation of risk in favour of a bank should also, in principle, lead to more competitive prices for the services offered. The question is whether the risk is appropriately allocated at present in the triangular relationship involving consumer, bank and merchant. We seek submissions on this issue. We will address any residual concerns from these issues in our third report.

### *Unauthorised EFT transactions*

305 In New Zealand, guidelines regarding customer liability for unauthorised EFT transactions can be found in the Code of Banking Practice (The Code), administered by the New Zealand Bankers' Association (NZBA), and the EFT Code of Practice, administered by the Ministry of Consumer Affairs. Formerly, member banks of the NZBA were signatories to the EFT Code, however in 1996 the NZBA decided to withdraw from the EFT Code and include its consumer liability provision in the Code of Banking Practice. Other providers of EFTPOS services (in effect, a small number of finance companies) remain bound by the EFT Code. Consumers whose EFT services are provided by banks have seen a shift in liability for unauthorised transactions in favour of the banks.[437]

306 The Code of Banking Practice covers member banks' dealings with individual customers, however the Statement of Principles relating to Small, Medium Size and Farming Businesses released by the NZBA in 1999 imports the provisions of the Code into these

---

[436] Similar problems arise regarding the responsibilities of the holder of an electronic signature to safeguard that signature from unauthorised use, which were discussed at the 35th session of the UNCITRAL Working Group on Electronic Commerce held in September 1999. The Working Group's report is available from www.uncitral.org. See discussion of draft article 9, paras 99–108.

[437] This section of the Banking chapter draws considerably on the writing of Professor Mark Sneddon, Special Counsel Electronic Commerce, Clayton Utz and Associate Professor of Law, University of Melbourne. In particular see "Risk Allocation in Electronic Banking: Lessons for Electronic Commerce", paper delivered at the New Zealand Law Society Conference, 1999.

dealings, with the exception of credit arrangements. Clause 5.5.3 of the Code provides that customers may be liable for loss arising from unauthorised transactions if they have *contributed to or caused* that loss (our emphasis). This places a heavy burden on the customer, especially when compared to the equivalent United Kingdom Code, under which a customer is only liable where they have acted fraudulently or been grossly negligent. In addition, the burden for proving gross negligence or fraud lies with the card issuer in the United Kingdom, whereas the New Zealand Code is silent as to where the burden of proof lies. While in practice, we are advised, the Banking Ombudsman would be unlikely to find against a customer who, for example, allowed another to observe him or her inputing a PIN in a shop, such conduct arguably constitutes "contributing to the loss".

307 A further example of the stringency of the New Zealand Code is the standard of care which the banks require their customers to take with regard to cards, PINs and passwords. Clause 5.5.3 (iii) imposes liability on the customer if loss is caused by keeping a written record of a PIN or password. Sneddon observes that the Australian Code only prohibits keeping a written record if the PIN or password is not reasonably disguised. Although ambiguous, the Australian standard is clearly not as onerous as the New Zealand one. As Sneddon observes many customers simply cannot remember a PIN and must record it.[438]

308 Another area of the Code which may expose customers to disproportionate liability is clause 5.5.6 which provides that where customers have contributed to the loss they may be liable for loss occurring before notification to the bank up to the daily transaction limit on the card or account(s). These limits have increased in recent years, from between $4–5000 up to $10 000 per account. As one card may access more than one account, and limits may include credit available on a loan facility, this provision of the Code exposes the customer to potentially enormous liability.

309 The Code is monitored by the Banking Ombudsman, and is due for a comprehensive public review by 1 November 2001 (five years since it came into force). In the Annual Report for 1997/8 the Banking Ombudsman notes that the use of credit and debit cards make up the majority of complaints regarding electronic banking services. During this period the Banking Ombudsman conducted the first investigation into a complaint relating to computer

[438] Above n 437, 39.

banking services.[439] Few complaints are received regarding telephone banking, although the low numbers of customers making use of these services (compared with other electronic services such as ATMs and EFTPOS) perhaps indicates a degree of caution on the consumer's behalf.

**Table 15.1: Number of complaints regarding electronic banking services[440]**

| Business area | 1995–6 | 1996–7 | 1997–8 |
|---|---|---|---|
| ATM | 6 (1%) | 17 (2%) | 19 (2%) |
| Credit/debit cards | 57 (10%) | 74 (11%) | 105 (13%) |
| All cases | 553 (100%) | 692 (100%) | 790 (100%) |

*Source*: Banking Ombudsman's Annual Report 1997/1998, 11, as n 432.

310 Sneddon makes the point that as the authentication system is chosen by the bank or financial institution, and is a "primitive and inherently insecure" procedure, then the institution should bear the risk of unauthorised use. He cites examples of more secure authentication methods which will undoubtedly become more prevalent, including digital signatures and biometric verification such as iris scanners and voice recognition (although notes that these are not yet cost effective for mass roll-out).[441]

311 These issues were considered by the Australian EFT Working Group in its *Discussion Paper on an Expanded EFT Code of Practice*.[442] The Group (which includes Professor Sneddon) concluded that liability should be shared between the institution and the customer, depending on the circumstances of the loss. Three options for allocation were proposed:

- adapt the existing code by refining the definition of a "reasonable attempt" to protect the security of a PIN;
- apportion liability to the institution unless it can affirmatively prove that the customer was fraudulent or grossly negligent (similar to United Kingdom and Danish models, and the European Commission's recommendations);

[439] Above n 432, 5.

[440] Above n 432, 11.

[441] Above n 437, 7.

[442] Available at www.asic.gov.au.

- apportion liability to the institution except where loss is caused by delays in reporting lost or stolen cards, or a failure to report unauthorised transactions appearing on statements (similar to United States Regulation E).

312 Similar issues arise here to those referred to in para 304. Similar arguments for the need to allocate risk in the bank's favour apply in this situation also. We invite submissions on whether:

- the existing allocation of risk set out in the Code of Banking Practice is appropriate given the various factors we have identified; and
- if not, what justifiable basis may exist for legislative action to cure any problems.

Our view is that the onus should be on those who seek to justify legislative intervention to demonstrate that this would be preferable to contractual arrangements. While our principle of private sector leadership is of some importance on this issue, we also note that consumer protection issues fall outside the scope of that principle as previously defined.[443]

---

[443] Para E3 and para 10.

# 16
# Securities

313 ELECTRONIC SYSTEMS HAVE TRANSFORMED the nature of securities transactions on a global scale. All shares in New Zealand companies listed on the New Zealand Stock Exchange (NZSE) are now traded in a paperless environment on the FASTER (Fully Automated Screen Trading and Electronic Registration) system. A description of the FASTER system follows below and is included for interest only. In ECom 1, we queried whether the Securities Act 1978 should be amended to give the Securities Commission jurisdiction over offers for securities made to the New Zealand public from overseas.[444] A corollary of this issue is what controls the Securities Commission should exercise over offers made from New Zealand but exclusively to people and institutions outside New Zealand.

314 In response to ECom 1, it was noted that although the Securities Act 1978 does not purport to apply to conduct outside New Zealand (unlike the Fair Trading Act 1986), the current effect of the Act is that it does apply to offers to the New Zealand public made from outside New Zealand. This is supported by case law and the existence of exemptions in the Securities Act 1978 for the case of overseas offerors.

315 Section 7 provides that certain sections of the Securities Act 1978 (notably those imposing disclosure requirements on offers made to the public) do not apply where an offer is made to persons outside New Zealand only, or to persons in New Zealand selected other than as members of the public. By exempting offers made to those outside New Zealand from certain sections of the Act, it follows that the remainder of the Act is intended to cover such offers. Thus the Act can be seen to apply extra territorially, and in *Society of Lloyds and Oxford Members Agency Limited v Hyslop*[445] Richardson J stated that this approach should also be applied to offers made

[444] See ECom 1, paras 382–383.

[445] [1993] 3 NZLR 135

from overseas to the New Zealand public. He observed that in relation to an investment made outside New Zealand:

> . . . section 7 itself provides for extra territorial application of the legislation and there is nothing in the statute to suggest a narrower approach in the present case.[446]

316 The Securities Commission makes the further point that if the Act does not extend to offers made from outside New Zealand there would be no need for overseas offerors to seek exemptions under the Act, yet the Act clearly provides for this in section 5(5).[447] The Securities Commission is considering a policy regarding overseas collective investments in general: that where an offer of securities is capable of being accepted by someone in New Zealand, then there is deemed to be sufficient activity for the Securities Act 1978 to apply to that offer. Similar approaches have been taken in Australia and the United States.

317 We concur with the Securities Commission that no reform is necessary in this respect.

### *Offers made from within New Zealand to overseas persons*

318 The effect of section 7 of the Securities Act 1978 is that the Securities Commission is unable to regulate advertisements for securities that are made from New Zealand exclusively to foreign jurisdictions. This may cause New Zealand to be viewed as a "safe" jurisdiction in which to base internet servers or web pages promoting offers of securities that are not subject to any regulatory regime. The Securities Commission considers that it is important that it is able to respond effectively to complaints regarding advertisements based in New Zealand that are likely to deceive, mislead, or confuse investors overseas. One way of achieving this would be to amend section 7 of the Act to provide that the Commission's powers in respect of advertisements under section 38(b) of the Act apply to offers made to persons inside or outside New Zealand. The Securities Commission has recommended to Government that such an amendment be made.

---

[446] Above n 445, 140.

[447] Currently exemptions have been granted in respect of Australian equity offers and unit trusts, other overseas companies listed on approved exchanges, and certain overseas companies undergoing restructuring and amalgamation.

### *The FASTER system*[448]

319 The system for the electronic transfer of securities on the NZSE became fully operational on 18 May 1998, when the Order in Council approving the FASTER system came into force. That order revoked an earlier Securities Transfer (Approval of FASTER System) Order 1992. Between 1992 and 1998 it was possible to conduct transactions electronically between two brokers, and between a buyer and its broker, but transactions between a seller and its broker required the manual transfer form and securities certificate. Now these transactions can also take place electronically. The requirement to issue certificates under section 55(4) of the Securities Act 1978 has been removed for overseas companies and issuers of securities other than shares. Under section 54(4), New Zealand companies whose shares could be transferred by an approved electronic system which does not require a share certificate were already exempt from having to send a certificate to the security holder within one month of allotment/transfer. FASTER interconnects the trading system, members' office systems, share registries and payments systems. All the New Zealand equities are currently traded through FASTER, and the system is expected to extend to New Zealand fixed interest instruments (eg bonds, debentures). Some but not all overseas equities are traded through the system, but unlisted (private) securities are not.

320 To effect a transaction two numbers are needed: the client's registry account number and their FASTER identification number (FIN), which is confidential and operates in a similar way to a banking PIN. When these numbers are combined with the unique code of the securities being bought or sold, the orders are matched and FASTER then notifies broker systems of the trades. Statements or contract notes must be sent to both parties within five working days of the transaction.

321 All settlements within FASTER occur using a system of simultaneous, final and irrevocable delivery versus payment (SFI DvP), so that real payments and irrevocable delivery occurs simultaneously. Until a transaction has settled, the securities are held by the brokers on trust for the clients (NZSE Regulations 17(8)). The securities are held in the broker's transfer account, through

---

[448] Information obtained from the New Zealand Stock Exchange Fact Book 1998, available at www.nzsc.co.nz, and "NZSE FASTER system operational" (1999) 499 LawTalk 6.

which all brokerage transfers must be cleared. Regulations 17(9) and (10) require brokers to deposit payments in respect of securities into the Members Clients Funds Account until the transfer is complete. Parties should therefore be protected against any default on behalf of a broker.

### *Internet trading*

322 Under section 7 of the Securities Transfer Act 1991 a securities transfer system which is partly or wholly electronic must be approved by the Minister of Commerce (acting on a recommendation from the Securities Commission). To date approval has only been given in respect of FASTER, and for the electronic transfer of securities issued by New Zealand companies and listed on the Australian Stock Exchange. It is not currently possible to transfer New Zealand securities over the internet, although the internet can and is used to communicate with brokers and place orders.[449]

323 Compared with other jurisdictions the New Zealand securities market is not heavily regulated. We do not consider that there are any legal barriers to the development of electronic trading which need to be addressed in this report.

---

[449] See further "If you want to get ahead, get online: investors embrace Internet trading" *The Independent*, 14 July 1999, 24.

# 17
# Intellectual property

324 In ECOM 1 we called for submissions on whether the laws which protect intellectual property needed to be reformed to cope with new forms of electronic communications and publishing.[450] The Ministry of Commerce is the government agency best placed to be developing policy in this area. We therefore propose not to go into further detail on intellectual property issues in this report, but to refer to the work being undertaken by the Ministry of Commerce.[451]

325 The issue of domain name registration and "cyber squatters", who use trademarks as domain names without authorisation, has been examined in the Ministry's Review of the Trademarks Act 1953. No changes to legislation were recommended in relation to domain name registration, as it was concluded that the courts are dealing adequately with the issues.[452]

326 The allocation of domain names raises wider issues of internet governance which are also being addressed by the Ministry of Commerce. The Ministry is supporting the initiatives of the Internet Society of New Zealand in its submissions to the International Corporation for Assigned Names and Numbers and the World Intellectual Property Organisation regarding the regulation of domain name registration, and the current "first in first served" approach taken in New Zealand.

327 Copyright raises a number of difficult issues within the electronic environment. The Ministry of Commerce intends to consider these issues in its strategic assessment of copyright law, completion of which is envisaged by June 2000. The submissions on ECom 1 queried how a number of problems would be approached, and we have provided the Ministry with a summary of these issues for consideration in the strategic assessment.

---

[450] See ECom 1, paras 365–381.

[451] Details confirmed by the Ministry of Commerce in correspondence dated 17 June 1999.

[452] Leading cases include *Oggi Advertising Ltd v McKenzie & Ors* [1999] 1 NZLR 631 (discussed in ECom 1, para 368) and *New Zealand Post Ltd v Leng* (1998) 8 TCLR 502.

# 18
# Taxation

328 In ECOM 1 we called for submissions on whether there was a case for special rules for the taxation of electronic transactions, and whether such issues should be addressed by the Law Commission or the Inland Revenue Department.[453] It seems evident that the Inland Revenue Department is the most appropriate agency to be forming policy in this area. We do not therefore propose to go into detail on taxation issues in this report, but do refer to the work being undertaken by the Inland Revenue Department.[454]

329 The Inland Revenue Department subscribes to an overall principle of neutrality, for example it does not discriminate between delivery mechanisms when taxing transactions. This principle is outlined in the Department's *Guidelines to Taxation and the Internet*.[455] Submissions received on ECom 1 strongly favoured the neutrality principle, and stressed the need to address the anomaly that software imported electronically is considered a service and not subject to GST, whereas GST is payable on the goods component of software imported physically.

330 This issue was addressed in the Discussion Paper *GST – A Review*[456] which proposes treating the copyright in software as a service, but copies of programs as goods which would attract GST. The proposal would not affect goods imported physically under section 12 of the Goods and Services Tax Act 1985. Submissions are being received on the Discussion Paper, and Inland Revenue is in the process of reporting to Government.

331 The Inland Revenue Department is supporting the work of the OECD and other international organisations in developing a consensus on taxation issues within the electronic environment.

---

[453] See ECom 1, paras 384–390.

[454] Details confirmed in correspondence with the Inland Revenue Department dated 18 June 1999.

[455] Available at http://www.ird.govt.nz/resource/taxaint/index.htm, 10 August 1999.

[456] Inland Revenue Department, Wellington, March 1999.

# 19
# Conclusions

## THE ELECTRONIC TRANSACTIONS ACT

332 **We recommend** that New Zealand enact an Electronic Transactions Act to remove the immediate barriers to electronic commerce (paras E4–E5, E12, 5, 7–8 and 23; and see generally the Model Law and the Australian Bill).

333 **We recommend** that the Electronic Transactions Act contain:

- equivalents to articles 4 (Party Autonomy), 5 (Non-Discrimination) and 5 *bis* (Incorporation by Reference) of the Model Law (see paragraph 62; paragraph 38 ECom 1; paragraphs 44–44-7 Guide to Enactment; Australian Bill, section 8).
- an equivalent to article 7 of the Model Law (Electronic Signatures) (see paragraphs 139–155; paragraphs 309–345 ECom 1; paragraphs 53–61 Guide to Enactment; Australian Bill, section 10);
- equivalents to clauses 11 (Production of Documents) and 12 (Retention of Documents) of the Australian Bill (see paragraphs 130–137; paragraphs 391–395 ECom 1; articles 8, 9 and 10 of the Model Law; paragraphs 62–69 and 72–75 Guide to Enactment).
- an equivalent to article 15 (Time and Place of Dispatch and Receipt of Data Messages) of the Model Law (see paragraphs 53–58; paragraphs 73, 90–93 ECom 1; paragraphs 100–109 Guide to Enactment; Australian Bill, section 14).
- a provision detailing that Internet Service Providers (ISPs) have no liability unless:
  - they have actual knowledge of the existence of information on the website which would be actionable at civil law or constitute a criminal offence; and
  - the ISP fails to remove promptly any offending information of which it has knowledge; and
  - that ISPs will not liable for reposting of information by a third party that has been previously removed unless it obtains

actual knowledge of such a reposting and fails to remove it promptly (see paragraph 260; chapter 4 ECom 1).

334 **We further recommend** that equivalents to clauses 11 and 12 of the Australian Bill, if enacted, are subject to the provisions of the proposed Evidence Code (see paragraphs 136–137 and 20; clause 13 Australian Bill; *Evidence: the Reform of the Law: NZLC R55* paragraphs 513–514).

335 **We recommend** that the Electronic Transactions Act and the proposed Evidence Code be enacted at the same time so that any immediate barriers to electronic commerce can be removed (see paragraphs 121–137).

336 **We recommend** that the Electronic Transactions Act **not** include:

- an equivalent of article 9 of the Model Law, as the admissibility of electronic documents is covered by the Evidence Code contained in NZLC R55 Volume 2, sections 117–123, which we are recommending be implemented through enactment of the Evidence Code;
- an equivalent of article 13 of the Model Law. We propose to revisit the desirability of enacting article 13 in our third report (see paragraphs 48–52; paragraphs 62, 94–99 ECom 1; paragraphs 83–92 Guide to Enactment);
- an equivalent of article 14 of the Model Law for the reasons given in paragraphs 59–60; paragraphs 93–99 Guide to Enactment;
- equivalents of articles 16 and 17 of the Model Law for the reasons given at paragraph 77 and chapter 4; paragraphs 100–136 ECom 1; paragraphs 108–122 Guide to Enactment.

337 **We recommend** that the Electronic Transactions Act applies to:

- electronic transactions conducted "in trade" (see paragraphs E8, 5, 34, 107; paragraphs 24–29 Guide to Enactment).
- consumer transactions (see paragraphs 108–114; paragraph 3 ECom 1; paragraphs 27 and 29 Guide to Enactment; Australian Bill, section 5 definition of "transaction" and sections 8(3) and (4) which provide for exemptions by regulation for specified transactions).

## MATTERS FOR OUR THIRD REPORT

338 **We recommend** that New Zealand continues to be represented at the UNCITRAL Working Group on Electronic Commerce. The possible adoption of Uniform Rules on Electronic Signatures arising

out of that work will be considered in our third report (see paragraphs 147–155).

339 **We recommend** that New Zealand continues to be represented at the Hague Conference on Private International Law. The merits of adopting outcomes from the Hague Conference will be considered in our third report (see paragraphs 279–283).

## OTHER RECOMMENDATIONS

340 **We recommend:**

- that a systematic review of all commercial legislation be undertaken by the government departments responsible for administering them, to ensure that the barriers to electronic commerce identified in chapter 5 (Statutory Overlay) are removed where appropriate (see paragraphs 92 and 101–102).
- that the definition of "distributor" in section 2(1) of the Defamation Act 1992 includes reference to an ISP (see paragraphs 264–270). Internet Service Providers should then be defined in a separate definition to include providers of the services discussed in paragraph 242.
- that the Reserve Bank should undertake review of the Financial Transactions Reporting Act 1996 in the near future to ensure fraudulent and other illegal activities involving electronic money are within the scope of that Act (see paragraphs 286–289 chapter 15 Banking).
- in relation to the delivery or services of notices and other documents, that such delivery or service take place electronically only where there has been prior consent on the part of the consumer in the manner stipulated in paragraphs 88–89, 93 and 110.
- that the Evidence Code be enacted contemporaneously with the proposed Electronic Transactions Act (see paragraphs 121 and 137).
- that the amendments to the Privacy Act 1993 recommended by the Privacy Commissioner be adopted (see paragraphs 175–177).
- that the four offences recommended in the *Computer Misuse* report be enacted. We also **recommend** that a fifth computer misuse offence be created; namely, intentionally and without authority gaining access to data stored in a computer. **We recommend** that this offence should have a maximum penalty of three years imprisonment. (See paragraphs 180–195 and *Computer Misuse* (NZLC R54 (1999)).

- that New Zealand monitors further international developments in respect of electronic transportation documents before making a final determination on whether legislation is necessary to implement articles 16 and 17 of the Model Law (see paragraph 77).

341 **We defer for consideration** in discrete reports:

- the possible abolition of the postal acceptance rule (see paragraphs 40–41);
- the merits of repealing the Contracts Enforcement Act (see paragraphs 46–47).

## FURTHER SUBMISSIONS

342 **We seek further submissions** on the following matters which will be addressed in our third report:

- In relation to the allocation of liability for unauthorised electronic banking transactions (both credit card and EFT transactions):
  - is the existing allocation set out in the Code of Banking Practice appropriate?;
  - if not, what are the bases for justifying legislative action to cure any problems? (See paragraphs 304 and 312.)
- In relation to the privacy issues raised by caching:
  - are there any practical problems and issues in the application of the existing law;
  - if so, do those problems arise in relation to collection, holding or giving access; and
  - if a law change is warranted, how that amendment might be framed? (See paragraphs 178 and 179.)
- In general on whether legislation is required to allow the use of electronic transportation documents (paragraph 78 and chapter 4 generally).
- We are of the view that there is not, as yet, a demonstrable need for legislative intervention to provide greater protection against the misuse of information. However, as there may be a demonstrable need in the near future for added protection, we seek further submissions on
  - 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 options are suggested to deal with the issues raised? (See paragraphs 201–238.)

---

# APPENDIX A

# Structure of government committees

A1 AN ELECTRONIC COMMERCE STEERING COMMITTEE was established to coordinate a work programme on electronic commerce issues. The Steering Committee is convened by the Ministry of Commerce. The membership of the Steering Committee is drawn from representatives of five sector committees which were established to consider specific electronic commerce issues.

**Electronic Commerce Steering Committee membership**

- Ministry of Commerce
- Ministry of Foreign Affairs and Trade
- Law Commission
- Ministry of Consumer Affairs
- Department of Prime Minister and Cabinet
- Inland Revenue Department
- the Treasury

A2 The Security Sector Committee considers issues to do with cryptography, authentication and electronic signatures, confidentiality and integrity of electronic communications, and hacking and computer security.

**Security Sector Committee membership**

- Department of Prime Minister and Cabinet
- Ministry of Justice
- Ministry of Commerce
- Police
- Security Agencies
- New Zealand Customs Service
- Ministry of Foreign Affairs and Trade

A3 The Revenue Based Interests Sector Committee examines the impact of electronic commerce on taxation and tariffs, with regard to the work being carried out by the OECD and other international forums.

**Revenue Based Interests Sector Committee membership**

- Inland Revenue Department
- New Zealand Customs Service
- Department of Internal Affairs
- Ministry of Commerce
- Ministry of Foreign Affairs and Trade
- the Treasury

A4 The Economic and Social Impacts Sector Committee considers trade issues, official statistics, electronic money, business capability and infrastructure, competition policy, and social impacts including education, employment and access.

**Economic and Social Impacts Sector Committee membership**

- Ministry of Foreign Affairs and Trade
- Ministry of Commerce
- the Treasury
- Inland Revenue Department
- Statistics New Zealand
- New Zealand Customs Service
- Department of Labour
- Ministry of Education
- Department of Social Welfare
- Department of Internal Affairs
- State Services Commission
- Ministry of Research, Science and Technology

A5 The Consumer Protection, Privacy and Property Sector Committee considers issues regarding the laws of contract and tort, choice of law and jurisdiction, evidence, consumer protection, law enforcement, privacy and intellectual property rights.

**Consumer Protection, Privacy and Property Sector Committee membership**

- Law Commission
- Ministry of Consumer Affairs

- Ministry of Commerce
- Ministry of Justice
- Office of the Privacy Commissioner
- Department of Internal Affairs
- New Zealand Customs Service
- Land Information New Zealand

A6 The Government Information Strategy Sector Committee is concerned with government operational use of electronic commerce including service delivery and compliance, and secure exchange of information. Currently this Committee is convened by the State Services Commission on an ad hoc basis.

---

APPENDIX B

# UNCITRAL Model Law on Electronic Commerce and Guide to Enactment 1996 with additional article 5 bis as adopted in 1998 by the United Nations

# CONTENTS

## Resolution adopted by the General Assembly

*[on the report of the Sixth Committee (A/51/628)]*

*51/162 Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law*

*The General Assembly,*

*Recalling* its resolution 2205 (XXI) of 17 December 1966, by which it created the United Nations Commission on International Trade Law, with a mandate to further the progressive harmonization and unification of the law of international trade and in that respect to bear in mind the interests of all peoples, in particular those of developing countries, in the extensive development of international trade,

*Noting* that an increasing number of transactions in international trade are carried out by means of electronic data interchange and other means of communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information,

*Recalling* the recommendation on the legal value of computer records adopted by the Commission at its eighteenth session, in 1985, (1) and paragraph 5(*b*) of General Assembly resolution 40/71 of 11 December 1985, in which the Assembly called upon Governments and international organizations to take action, where appropriate, in conformity with the recommendation of the Commission,[1] so as to ensure legal security in the context of the widest possible use of automated data processing in international trade,

*Convinced* that the establishment of a model law facilitating the use of electronic commerce that is acceptable to States with different legal, social and economic systems, could contribute significantly to the development of harmonious international economic relations,

*Noting* that the Model Law on Electronic Commerce was adopted by the Commission at its twenty-ninth session after consideration of the observations of Governments and interested organizations,

---

1 See *Official Records of the General Assembly, Fortieth Session, Supplement No. 17* (A/40/17), chap. VI, sect. B.

*Believing* that the adoption of the Model Law on Electronic Commerce by the Commission will assist all States significantly in enhancing their legislation governing the use of alternatives to paper-based methods of communication and storage of information and in formulating such legislation where none currently exists,

1 *Expresses* its appreciation to the United Nations Commission on International Trade Law for completing and adopting the Model Law on Electronic Commerce contained in the annex to the present resolution and for preparing the Guide to Enactment of the Model Law;

2 *Recommends* that all States give favourable consideration to the Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information;

3 *Recommends* also that all efforts be made to ensure that the Model Law, together with the Guide, become generally known and available.

*85th plenary meeting*
*16 December 1996*

# UNCITRAL Model Law on Electronic Commerce

*[Original: Arabic, Chinese, English, French, Russian, Spanish]*

## Part one. Electronic commerce in general

### Chapter I. General provisions

#### *Article 1. Sphere of application**

This Law** applies to any kind of information in the form of a data message used in the context*** of commercial**** activities.

#### *Article 2. Definitions*

For the purposes of this Law:

*(a)* "Data message" means information generated, sent, received or stored by electronic, optical or similar means including,

---

* The Commission suggests the following text for States that might wish to limit the applicability of this Law to international data messages:

"This Law applies to a data message as defined in paragraph (1) of article 2 where the data message relates to international commerce."

** This Law 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 to any kind of information in the form of a data message, 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

but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;

*(b)* "Electronic data interchange (EDI)" means the electronic transfer from computer to computer of information using an agreed standard to structure the information;

*(c)* "Originator" of a data message means a person by whom, or on whose behalf, the data message purports to have been sent or generated prior to storage, if any, but it does not include a person acting as an intermediary with respect to that data message;

*(d)* "Addressee" of a data message means a person who is intended by the originator to receive the data message, but does not include a person acting as an intermediary with respect to that data message;

*(e)* "Intermediary", with respect to a particular data message, means a person who, on behalf of another person, sends, receives or stores that data message or provides other services with respect to that data message;

*(f)* "Information system" means a system for generating, sending, receiving, storing or otherwise processing data messages.

*Article 3. 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 4. Variation by agreement*

(1) As between parties involved in generating, sending, receiving, storing or otherwise processing data messages, and except as otherwise provided, the provisions of chapter III may be varied by agreement.

(2) Paragraph (1) does not affect any right that may exist to modify by agreement any rule of law referred to in chapter II.

## Chapter II. Application of legal requirements to data messages

### *Article 5. Legal recognition of data messages*

Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

### *Article 5 bis. Incorporation by reference*

(as adopted by the Commission at its thirty-first session, in June 1998)

Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is not contained in the data message purporting to give rise to such legal effect, but is merely referred to in that data message.

### *Article 6. Writing*

(1) Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.

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

### *Article 7. Signature*

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

*(a)* a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

*(b)* that method 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 therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

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

*Article 8. Original*

(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:

*(a)* there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

*(b)* where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.

(3) For the purposes of subparagraph (a) of paragraph (1):

*(a)* the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

*(b)* the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

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

*Article 9. Admissibility and evidential weight of data messages*

(1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:

*(a)* on the sole ground that it is a data message; or,

*(b)* if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in

which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.

*Article 10. Retention of data messages*

(1) Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:

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

*(b)* the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

*(c)* such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.

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

(3) A person may satisfy the requirement referred to in paragraph (1) by using the services of any other person, provided that the conditions set forth in subparagraphs (a), (b) and (c) of paragraph (1) are met.

## Chapter III. Communication of data messages

*Article 11. Formation and validity of contracts*

(1) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.

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

*Article 12. Recognition by parties of data messages*

(1) As between the originator and the addressee of a data message, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

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

*Article 13. Attribution of data messages*

(1) A data message is that of the originator if it was sent by the originator itself.

(2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:

*(a)* by a person who had the authority to act on behalf of the originator in respect of that data message; or

*(b)* by an information system programmed by, or on behalf of, the originator to operate automatically.

(3) As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if:

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

*(b)* the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.

(4) Paragraph (3) does not apply:

*(a)* as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or

*(b)* in a case within paragraph (3)*(b)*, at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.

(5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee,

the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.

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

*Article 14. Acknowledgement of receipt*

(1) Paragraphs (2) to (4) of this article apply where, on or before sending a data message, or by means of that data message, the originator has requested or has agreed with the addressee that receipt of the data message be acknowledged.

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

*(a)* any communication by the addressee, automated or otherwise,

or

*(b)* any conduct of the addressee,

sufficient to indicate to the originator that the data message has been received.

(3) Where the originator has stated that the data message is conditional on receipt of the acknowledgement, the data message is treated as though it has never been sent, until the acknowledgement is received.

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

*(a)* may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

*(b)* if the acknowledgement is not received within the time specified in subparagraph (a), may, upon notice to the addressee, treat the data message as though it had never been sent, or exercise any other rights it may have.

(5) Where the originator receives the addressee's acknowledgement of receipt, it is presumed that the related data message was received by the addressee. That presumption does not imply that the data message corresponds to the message received.

(6) Where the received acknowledgement states that the related data message met technical requirements, either agreed upon or set forth in applicable standards, it is presumed that those requirements have been met.

(7) Except in so far as it relates to the sending or receipt of the data message, this article is not intended to deal with the legal consequences that may flow either from that data message or from the acknowledgement of its receipt.

*Article 15. Time and place of dispatch and receipt of data messages*

(1) Unless otherwise agreed between the originator and the addressee, the dispatch of a data message occurs when it enters an information system outside the control of the originator or of the person who sent the data message on behalf of the originator.

(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows:

*(a)* if the addressee has designated an information system for the purpose of receiving data messages, receipt occurs:

(i) at the time when the data message enters the designated information system; or

(ii) if the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is retrieved by the addressee;

*(b)* if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.

(3) Paragraph (2) applies notwithstanding that the place where the information system is located may be different from the place where the data message is deemed to be received under paragraph (4).

(4) Unless otherwise agreed between the originator and the addressee, a data message is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business. For the purposes of this paragraph:

*(a)* if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business;

*(b)* if the originator or the addressee does not have a place of business, reference is to be made to its habitual residence.

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

## Part two. Electronic commerce in specific areas

### CHAPTER I. CARRIAGE OF GOODS

*Article 16. Actions related to contracts of carriage of goods*

Without derogating from the provisions of part one of this Law, this chapter applies to any action in connection with, or in pursuance of, a contract of carriage of goods, including but not limited to:

*(a)* (i) furnishing the marks, number, quantity or weight of goods;
(ii) stating or declaring the nature or value of goods;
(iii) issuing a receipt for goods;
(iv) confirming that goods have been loaded;

*(b)* (i) notifying a person of terms and conditions of the contract;
(ii) giving instructions to a carrier;

*(c)* (i) claiming delivery of goods;
(ii) authorizing release of goods;
(iii) giving notice of loss of, or damage to, goods;

*(d)* giving any other notice or statement in connection with the performance of the contract;

*(e)* undertaking to deliver goods to a named person or a person authorized to claim delivery;

*(f)* granting, acquiring, renouncing, surrendering, transferring or negotiating rights in goods;

*(g)* acquiring or transferring rights and obligations under the contract.

*Article 17. Transport documents*

(1) Subject to paragraph (3), where the law requires that any action referred to in article 16 be carried out in writing or by using a paper document, that requirement is met if the action is carried out by using one or more data messages.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for failing either to carry out the action in writing or to use a paper document.

(3) If a right is to be granted to, or an obligation is to be acquired by, one person and no other person, and if the law requires that, in order to effect this, the right or obligation must be conveyed to that person by the transfer, or use of, a paper document, that requirement is met if the right or obligation is conveyed by using one or more data messages, provided that a reliable method is used to render such data message or messages unique.

(4) For the purposes of paragraph (3), the standard of reliability required shall be assessed in the light of the purpose for which the right or obligation was conveyed and in the light of all the circumstances, including any relevant agreement.

(5) Where one or more data messages are used to effect any action in subparagraphs *(f)* and *(g)* of article 16, no paper document used to effect any such action is valid unless the use of data messages has been terminated and replaced by the use of paper documents. A paper document issued in these circumstances shall contain a statement of such termination. The replacement of data messages by paper documents shall not affect the rights or obligations of the parties involved.

(6) If a rule of law is compulsorily applicable to a contract of carriage of goods which is in, or is evidenced by, a paper document, that rule shall not be inapplicable to such a contract of carriage of goods which is evidenced by one or more data messages by reason of the fact that the contract is evidenced by such data message or messages instead of by a paper document.

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

# Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)

## PURPOSE OF THIS GUIDE

1. In preparing and adopting the UNCITRAL Model Law on Electronic Commerce (hereinafter referred to as "the Model Law"), the United Nations Commission on International Trade Law (UNCITRAL) was mindful that the Model Law would be a more effective tool for States modernizing their legislation if background and explanatory information would be provided to executive branches of Governments and legislators to assist them in using the Model Law. The Commission was also aware of the likelihood that the Model Law would be used in a number of States with limited familiarity with the type of communication techniques considered in the Model Law. This Guide, much of which is drawn from the *travaux préparatoires* of the Model Law, is also intended to be helpful to users of electronic means of communication as well as to scholars in that area. In the preparation of the Model Law, it was assumed that the draft Model Law would be accompanied by such a guide. For example, it was decided in respect of a number of issues not to settle them in the draft Model Law but to address them in the Guide so as to provide guidance to States enacting the draft Model Law. The information presented in this Guide is intended to explain why the provisions in the Model Law have been included as essential basic features of a statutory device designed to achieve the objectives of the Model Law. Such information might assist States also in considering which, if any, of the provisions of the Model Law might have to be varied to take into account particular national circumstances.

## I. INTRODUCTION TO THE MODEL LAW

### *A. Objectives*

2. The use of modern means of communication such as electronic mail and electronic data interchange (EDI) for the conduct of international trade transactions has been increasing rapidly and is expected to develop further as technical supports such as information highways and the INTERNET become more widely accessible. However, the communication of legally significant information in the form of paperless messages may be hindered by legal obstacles to the use of such messages, or by uncertainty as to their legal effect or validity. The purpose of the Model Law is to offer national legislators a set of internationally acceptable rules as to how a number of such legal obstacles may be removed, and how a more secure legal environment may be created for what has become known as "electronic commerce". The principles expressed in the Model Law are also intended to be of use to individual users of electronic commerce in the drafting of some of the contractual solutions that might be needed to overcome the legal obstacles to the increased use of electronic commerce.

3. The decision by UNCITRAL to formulate model legislation on electronic commerce was taken in response to the fact that in a number of countries the existing legislation governing communication and storage of information is inadequate or outdated because it does not contemplate the use of electronic commerce. In certain cases, existing legislation imposes or implies restrictions on the use of modern means of communication, for example by prescribing the use of "written", "signed" or "original" documents. While a few countries have adopted specific provisions to deal with certain aspects of electronic commerce, there exists no legislation dealing with electronic commerce as a whole. This may result in uncertainty as to the legal nature and validity of information presented in a form other than a traditional paper document. Moreover, while sound laws and practices are necessary in all countries where the use of EDI and electronic mail is becoming widespread, this need is also felt in many countries with respect to such communication techniques as telecopy and telex.

4. The Model Law may also help to remedy disadvantages that stem from the fact that inadequate legislation at the national level creates obstacles to international trade, a significant amount of which is linked to the use of modern communication techniques. Disparities among, and uncertainty about, national legal regimes governing the use of such communication techniques may

contribute to limiting the extent to which businesses may access international markets.

5. Furthermore, at an international level, the Model Law may be useful in certain cases as a tool for interpreting existing international conventions and other international instruments that create legal obstacles to the use of electronic commerce, for example by prescribing that certain documents or contractual clauses be made in written form. As between those States parties to such international instruments, the adoption of the Model Law as a rule of interpretation might provide the means to recognize the use of electronic commerce and obviate the need to negotiate a protocol to the international instrument involved.

6. The objectives of the Model Law, which include enabling or facilitating the use of electronic commerce and providing equal treatment to users of paper-based documentation and to users of computer-based information, are essential for fostering economy and efficiency in international trade. By incorporating the procedures prescribed in the Model Law in its national legislation for those situations where parties opt to use electronic means of communication, an enacting State would create a media-neutral environment.

### *B. Scope*

7. The title of the Model Law refers to "electronic commerce". While a definition of "electronic data interchange (EDI)" is provided in article 2, the Model Law does not specify the meaning of "electronic commerce". In preparing the Model Law, the Commission decided that, in addressing the subject matter before it, it would have in mind a broad notion of EDI, covering a variety of trade-related uses of EDI that might be referred to broadly under the rubric of "electronic commerce" (see A/CN.9/360, paras. 28–29), although other descriptive terms could also be used. Among the means of communication encompassed in the notion of "electronic commerce" are the following modes of transmission based on the use of electronic techniques: communication by means of EDI defined narrowly as the computer-to-computer transmission of data in a standardized format; transmission of electronic messages involving the use of either publicly available standards or proprietary standards; transmission of free-formatted text by electronic means, for example through the INTERNET. It was also noted that, in certain circumstances, the notion of "electronic

commerce" might cover the use of techniques such as telex and telecopy.

8. It should be noted that, while the Model Law was drafted with constant reference to the more modern communication techniques, e.g., EDI and electronic mail, the principles on which the Model Law is based, as well as its provisions, are intended to apply also in the context of less advanced communication techniques, such as telecopy. There may exist situations where digitalized information initially dispatched in the form of a standardized EDI message might, at some point in the communication chain between the sender and the recipient, be forwarded in the form of a computer-generated telex or in the form of a telecopy of a computer print-out. A data message may be initiated as an oral communication and end up in the form of a telecopy, or it may start as a telecopy and end up as an EDI message. A characteristic of electronic commerce is that it covers programmable messages, the computer programming of which is the essential difference between such messages and traditional paper-based documents. Such situations are intended to be covered by the Model Law, based on a consideration of the users' need for a consistent set of rules to govern a variety of communication techniques that might be used interchangeably. More generally, it may be noted that, as a matter of principle, no communication technique is excluded from the scope of the Model Law since future technical developments need to be accommodated.

9. The objectives of the Model Law are best served by the widest possible application of the Model Law. Thus, although there is provision made in the Model Law for exclusion of certain situations from the scope of articles 6, 7, 8, 11, 12, 15 and 17, an enacting State may well decide not to enact in its legislation substantial restrictions on the scope of application of the Model Law.

10. The Model Law should be regarded as a balanced and discrete set of rules, which are recommended to be enacted as a single statute. Depending on the situation in each enacting State, however, the Model Law could be implemented in various ways, either as a single statute or in several pieces of legislation (see below, para. 143).

### C. *Structure*

11. The Model Law is divided into two parts, one dealing with electronic commerce in general and the other one dealing with electronic commerce in specific areas. It should be noted that part two of the Model Law, which deals with electronic commerce in

specific areas, is composed of a chapter I only, dealing with electronic commerce as it applies to the carriage of goods. Other aspects of electronic commerce might need to be dealt with in the future, and the Model Law can be regarded as an open-ended instrument, to be complemented by future work.

12. UNCITRAL intends to continue monitoring the technical, legal and commercial developments that underline the Model Law. It might, should it regard it advisable, decide to add new model provisions to the Model Law or modify the existing ones.

### *D. A "framework" law to be supplemented by technical regulations*

13. The Model Law is intended to provide essential procedures and principles for facilitating the use of modern techniques for recording and communicating information in various types of circumstances. However, it is a "framework" law that does not itself set forth all the rules and regulations that may be necessary to implement those techniques in an enacting State. Moreover, the Model Law is not intended to cover every aspect of the use of electronic commerce. Accordingly, an enacting State may wish to issue regulations to fill in the procedural details for procedures authorized by the Model Law and to take account of the specific, possibly changing, circumstances at play in the enacting State, without compromising the objectives of the Model Law. It is recommended that, should it decide to issue such regulation, an enacting State should give particular attention to the need to maintain the beneficial flexibility of the provisions in the Model Law.

14. It should be noted that the techniques for recording and communicating information considered in the Model Law, beyond raising matters of procedure that may need to be addressed in the implementing technical regulations, may raise certain legal questions the answers to which will not necessarily be found in the Model Law, but rather in other bodies of law. Such other bodies of law may include, for example, the applicable administrative, contract, criminal and judicial-procedure law, which the Model Law is not intended to deal with.

### *E. The "functional-equivalent" approach*

15. The Model Law is based on the recognition that legal requirements prescribing the use of traditional paper-based documentation constitute the main obstacle to the development of modern means of communication. In the preparation of the

Model Law, consideration was given to the possibility of dealing with impediments to the use of electronic commerce posed by such requirements in national laws by way of an extension of the scope of such notions as "writing", "signature" and "original", with a view to encompassing computer-based techniques. Such an approach is used in a number of existing legal instruments, e.g., article 7 of the UNCITRAL Model Law on International Commercial Arbitration and article 13 of the United Nations Convention on Contracts for the International Sale of Goods. It was observed that the Model Law should permit States to adapt their domestic legislation to developments in communications technology applicable to trade law without necessitating the wholesale removal of the paper-based requirements themselves or disturbing the legal concepts and approaches underlying those requirements. At the same time, it was said that the electronic fulfilment of writing requirements might in some cases necessitate the development of new rules. This was due to one of many distinctions between EDI messages and paper-based documents, namely, that the latter were readable by the human eye, while the former were not so readable unless reduced to paper or displayed on a screen.

16. The Model Law thus relies on a new approach, sometimes referred to as the "functional equivalent approach", which is based on an analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic-commerce techniques. For example, among the functions served by a paper document are the following: to provide that a document would be legible by all; to provide that a document would remain unaltered over time; to allow for the reproduction of a document so that each party would hold a copy of the same data; to allow for the authentication of data by means of a signature; and to provide that a document would be in a form acceptable to public authorities and courts. It should be noted that in respect of all of the above-mentioned functions of paper, electronic records can provide the same level of security as paper and, in most cases, a much higher degree of reliability and speed, especially with respect to the identification of the source and content of the data, provided that a number of technical and legal requirements are met. However, the adoption of the functional-equivalent approach should not result in imposing on users of electronic commerce more stringent standards of security (and the related costs) than in a paper-based environment.

17. A data message, in and of itself, cannot be regarded as an equivalent of a paper document in that it is of a different nature

and does not necessarily perform all conceivable functions of a paper document. That is why the Model Law adopted a flexible standard, taking into account the various layers of existing requirements in a paper-based environment: when adopting the "functional-equivalent" approach, attention was given to the existing hierarchy of form requirements, which provides distinct levels of reliability, traceability and unalterability with respect to paper-based documents. For example, the requirement that data be presented in written form (which constitutes a "threshold requirement") is not to be confused with more stringent requirements such as "signed writing", "signed original" or "authenticated legal act".

18. The Model Law does not attempt to define a computer-based equivalent to any kind of paper document. Instead, it singles out basic functions of paper-based form requirements, with a view to providing criteria which, once they are met by data messages, enable such data messages to enjoy the same level of legal recognition as corresponding paper documents performing the same function. It should be noted that the functional-equivalent approach has been taken in articles 6 to 8 of the Model Law with respect to the concepts of "writing", "signature" and "original" but not with respect to other legal concepts dealt with in the Model Law. For example, article 10 does not attempt to create a functional equivalent of existing storage requirements.

### *F. Default rules and mandatory law*

19. The decision to undertake the preparation of the Model Law was based on the recognition that, in practice, solutions to most of the legal difficulties raised by the use of modern means of communication are sought within contracts. The Model Law embodies the principle of party autonomy in article 4 with respect to the provisions contained in chapter III of part one. Chapter III of part one contains a set of rules of the kind that would typically be found in agreements between parties, e.g., interchange agreements or "system rules". It should be noted that the notion of "system rules" might cover two different categories of rules, namely, general terms provided by communication networks and specific rules that might be included in those general terms to deal with bilateral relationships between originators and addressees of data messages. Article 4 (and the notion of "agreement" therein) is intended to encompass both categories of "system rules".

20. The rules contained in chapter III of part one may be used by parties as a basis for concluding such agreements. They may also

be used to supplement the terms of agreements in cases of gaps or omissions in contractual stipulations. In addition, they may be regarded as setting a basic standard for situations where data messages are exchanged without a previous agreement being entered into by the communicating parties, e.g., in the context of open-networks communications.

21. The provisions contained in chapter II of part one are of a different nature. One of the main purposes of the Model Law is to facilitate the use of modern communication techniques and to provide certainty with the use of such techniques where obstacles or uncertainty resulting from statutory provisions could not be avoided by contractual stipulations. The provisions contained in chapter II may, to some extent, be regarded as a collection of exceptions to well-established rules regarding the form of legal transactions. Such well-established rules are normally of a mandatory nature since they generally reflect decisions of public policy. The provisions contained in chapter II should be regarded as stating the minimum acceptable form requirement and are, for that reason, of a mandatory nature, unless expressly stated otherwise in those provisions. The indication that such form requirements are to be regarded as the "minimum acceptable" should not, however, be construed as inviting States to establish requirements stricter than those contained in the Model Law.

### *G. Assistance from UNCITRAL secretariat*

22. In line with its training and assistance activities, the UNCITRAL secretariat may provide technical consultations for Governments preparing legislation based on the UNCITRAL Model Law on Electronic Commerce, as it may for Governments considering legislation based on other UNCITRAL model laws, or considering adhesion to one of the international trade law conventions prepared by UNCITRAL.

23. Further information concerning the Model Law as well as the Guide and other model laws and conventions developed by UNCITRAL, may be obtained from the secretariat at the address below. The secretariat welcomes comments concerning the Model Law and the Guide, as well as information concerning enactment of legislation based on the Model Law.

International Trade Law Branch
Office of Legal Affairs
United Nations Vienna International Centre
P.O. Box 500
A-1400, Vienna, Austria

Telephone: (43-1) 26060-4060 or 4061
Telefax: (43-1) 26060-5813 or (43-1) 2692669
Telex: 135612 uno a
E-mail: uncitral@unov.un.or.at
Internet Home Page: http://www.un.or.at/uncitral

---

## II. ARTICLE-BY-ARTICLE REMARKS

# Part one. Electronic commerce in general

## Chapter I. General provisions

### *Article 1. Sphere of application*

24. The purpose of article 1, which is to be read in conjunction with the definition of "data message" in article 2*(a)*, is to delineate the scope of application of the Model Law. The approach used in the Model Law is to provide in principle for the coverage of all factual situations where information is generated, stored or communicated, irrespective of the medium on which such information may be affixed. It was felt during the preparation of the Model Law that exclusion of any form or medium by way of a limitation in the scope of the Model Law might result in practical difficulties and would run counter to the purpose of providing truly "media-neutral" rules. However, the focus of the Model Law is on "paperless" means of communication and, except to the extent expressly provided by the Model Law, the Model Law is not intended to alter traditional rules on paper-based communications.

25. Moreover, it was felt that the Model Law should contain an indication that its focus was on the types of situations encountered in the commercial area and that it had been prepared against the background of trade relationships. For that reason, article 1 refers to "commercial activities" and provides, in footnote ****, indications as to what is meant thereby. Such indications, which may be particularly useful for those countries where there does not exist a discrete body of commercial law, are modelled, for reasons of consistency, on the footnote to article 1 of the

UNCITRAL Model Law on International Commercial Arbitration. In certain countries, the use of footnotes in a statutory text would not be regarded as acceptable legislative practice. National authorities enacting the Model Law might thus consider the possible inclusion of the text of footnotes in the body of the Law itself.

26. The Model Law applies to all kinds of data messages that might be generated, stored or communicated, and nothing in the Model Law should prevent an enacting State from extending the scope of the Model Law to cover uses of electronic commerce outside the commercial sphere. For example, while the focus of the Model Law is not on the relationships between users of electronic commerce and public authorities, the Model Law is not intended to be inapplicable to such relationships. Footnote *** provides for alternative wordings, for possible use by enacting States that would consider it appropriate to extend the scope of the Model Law beyond the commercial sphere.

27. Some countries have special consumer protection laws that may govern certain aspects of the use of information systems. With respect to such consumer legislation, as was the case with previous UNCITRAL instruments (e.g., the UNCITRAL Model Law on International Credit Transfers), it was felt that an indication should be given that the Model Law had been drafted without special attention being given to issues that might arise in the context of consumer protection. At the same time, it was felt that there was no reason why situations involving consumers should be excluded from the scope of the Model Law by way of a general provision, particularly since the provisions of the Model Law might be found appropriate for consumer protection, depending on legislation in each enacting State. Footnote ** thus recognizes that any such consumer protection law may take precedence over the provisions in the Model Law. Legislators may wish to consider whether the piece of legislation enacting the Model Law should apply to consumers. The question of which individuals or corporate bodies would be regarded as "consumers" is left to applicable law outside the Model Law.

28. Another possible limitation of the scope of the Model Law is contained in the first footnote. In principle, the Model Law applies to both international and domestic uses of data messages. Footnote * is intended for use by enacting States that might wish to limit the applicability of the Model Law to international cases. It indicates a possible test of internationality for use by those States as a possible criterion for distinguishing international cases from

domestic ones. It should be noted, however, that in some jurisdictions, particularly in federal States, considerable difficulties might arise in distinguishing international trade from domestic trade. The Model Law should not be interpreted as encouraging enacting States to limit its applicability to international cases.

29. It is recommended that application of the Model Law be made as wide as possible. Particular caution should be used in excluding the application of the Model Law by way of a limitation of its scope to international uses of data messages, since such a limitation may be seen as not fully achieving the objectives of the Model Law. Furthermore, the variety of procedures available under the Model Law (particularly articles 6 to 8) to limit the use of data messages if necessary (e.g., for purposes of public policy) may make it less necessary to limit the scope of the Model Law. As the Model Law contains a number of articles (articles 6, 7, 8, 11, 12 , 15 and 17) that allow a degree of flexibility to enacting States to limit the scope of application of specific aspects of the Model Law, a narrowing of the scope of application of the text to international trade should not be necessary. Moreover, dividing communications in international trade into purely domestic and international parts might be difficult in practice. The legal certainty to be provided by the Model Law is necessary for both domestic and international trade, and a duality of regimes governing the use of electronic means of recording and communication of data might create a serious obstacle to the use of such means.

*References*[1]

A/50/17, paras. 213–219; A/CN.9/407, paras. 37–40; A/CN.9/406, paras. 80–85; A/CN.9/WG.IV/WP.62, article 1; A/CN.9/390, paras. 21–43; A/CN.9/WG.IV/WP.60, article 1; A/CN.9/387, paras. 15–28; A/CN.9/WG.IV/WP.57, article 1; A/CN.9/373, paras. 21–25 and 29–33; A/CN.9/WG.IV/WP.55, paras. 15–20.

---

[1] Reference materials listed by symbols in this Guide belong to the following three categories of documents:

A/50/17 and A/51/17 are the reports of UNCITRAL to the General Assembly on the work of its twenty-eighth and twenty-ninth sessions, held in 1995 and 1996, respectively;

A/CN.9/. . . documents are reports and notes discussed by UNCITRAL in the context of its annual session, including reports presented by the Working Group to the Commission;

A/CN.9/WG.IV/. . . documents are working papers considered by the UNCITRAL Working Group on Electronic Commerce (formerly known as the UNCITRAL Working Group on Electronic Data Interchange) in the preparation of the Model Law.

*"Data message"*

30. The notion of "data message" is not limited to communication but is also intended to encompass computer-generated records that are not intended for communication. Thus, the notion of "message" includes the notion of "record". However, a definition of "record" in line with the characteristic elements of "writing" in article 6 may be added in jurisdictions where that would appear to be necessary.

31. The reference to "similar means" is intended to reflect the fact that the Model Law was not intended only for application in the context of existing communication techniques but also to accommodate foreseeable technical developments. The aim of the definition of "data message" is to encompass all types of messages that are generated, stored, or communicated in essentially paperless form. For that purpose, all means of communication and storage of information that might be used to perform functions parallel to the functions performed by the means listed in the definition are intended to be covered by the reference to "similar means", although, for example, "electronic" and "optical" means of communication might not be, strictly speaking, similar. For the purposes of the Model Law, the word "similar" connotes "functionally equivalent".

32. The definition of "data message" is also intended to cover the case of revocation or amendment. A data message is presumed to have a fixed information content but it may be revoked or amended by another data message.

*"Electronic Data Interchange (EDI)"*

33. The definition of EDI is drawn from the definition adopted by the Working Party on Facilitation of International Trade Procedures (WP.4) of the Economic Commission for Europe, which is the United Nations body responsible for the development of UN/EDIFACT technical standards.

34. The Model Law does not settle the question whether the definition of EDI necessarily implies that EDI messages are communicated electronically from computer to computer, or whether that definition, while primarily covering situations where data messages are communicated through a telecommunications system, would also cover exceptional or incidental types of situation

where data structured in the form of an EDI message would be communicated by means that do not involve telecommunications systems, for example, the case where magnetic disks containing EDI messages would be delivered to the addressee by courier. However, irrespective of whether digital data transferred manually is covered by the definition of "EDI", it should be regarded as covered by the definition of "data message" under the Model Law.

*"Originator" and "Addressee"*

35. In most legal systems, the notion of "person" is used to designate the subjects of rights and obligations and should be interpreted as covering both natural persons and corporate bodies or other legal entities. Data messages that are generated automatically by computers without direct human intervention are intended to be covered by subparagraph *(c)*. However, the Model Law should not be misinterpreted as allowing for a computer to be made the subject of rights and obligations. Data messages that are generated automatically by computers without direct human intervention should be regarded as "originating" from the legal entity on behalf of which the computer is operated. Questions relevant to agency that might arise in that context are to be settled under rules outside the Model Law.

36. The "addressee" under the Model Law is the person with whom the originator intends to communicate by transmitting the data message, as opposed to any person who might receive, forward or copy the data message in the course of transmission. The "originator" is the person who generated the data message even if that message was transmitted by another person. The definition of "addressee" contrasts with the definition of "originator", which is not focused on intent. It should be noted that, under the definitions of "originator" and "addressee" in the Model Law, the originator and the addressee of a given data message could be the same person, for example in the case where the data message was intended for storage by its author. However, the addressee who stores a message transmitted by an originator is not itself intended to be covered by the definition of "originator".

37. The definition of "originator" should cover not only the situation where information is generated and communicated, but also the situation where such information is generated and stored without being communicated. However, the definition of "originator" is intended to eliminate the possibility that a recipient who merely stores a data message might be regarded as an originator.

*"Intermediary"*

38. The focus of the Model Law is on the relationship between the originator and the addressee, and not on the relationship between either the originator or the addressee and any intermediary. However, the Model Law does not ignore the paramount importance of intermediaries in the field of electronic communications. In addition, the notion of "intermediary" is needed in the Model Law to establish the necessary distinction between originators or addressees and third parties.

39. The definition of "intermediary" is intended to cover both professional and non-professional intermediaries, i.e., any person (other than the originator and the addressee) who performs any of the functions of an intermediary. The main functions of an intermediary are listed in subparagraph *(e)*, namely receiving, transmitting or storing data messages on behalf of another person. Additional "value-added services" may be performed by network operators and other intermediaries, such as formatting, translating, recording, authenticating, certifying and preserving data messages and providing security services for electronic transactions. "Intermediary" under the Model Law is defined not as a generic category but with respect to each data message, thus recognizing that the same person could be the originator or addressee of one data message and an intermediary with respect to another data message. The Model Law, which is focused on the relationships between originators and addressees, does not, in general, deal with the rights and obligations of intermediaries.

*"Information system"*

40. The definition of "information system" is intended to cover the entire range of technical means used for transmitting, receiving and storing information. For example, depending on the factual situation, the notion of "information system" could be indicating a communications network, and in other instances could include an electronic mailbox or even a telecopier. The Model Law does not address the question of whether the information system is located on the premises of the addressee or on other premises, since location of information systems is not an operative criterion under the Model Law.

*References*

A/51/17, paras. 116–138;
A/CN.9/407, paras. 41–52;
A/CN.9/406, paras. 132–156; A/CN.9/WG.IV/WP.62, article 2;
A/CN.9/390, paras. 44–65; A/CN.9/WG.IV/WP.60, article 2;
A/CN.9/387, paras. 29–52; A/CN.9/WG.IV/WP.57, article 2;
A/CN.9/373, paras. 11–20, 26–28 and 35–36; A/CN.9/WG.IV/WP.55, paras. 23–26;
A/CN.9/360, paras. 29–31; A/CN.9/WG.IV/WP.53, paras. 25–33.

*Article 3. Interpretation*

41. Article 3 is inspired by article 7 of the United Nations Convention on Contracts for the International Sale of Goods. It is intended to provide guidance for interpretation of the Model Law by courts and other national or local authorities. The expected effect of article 3 is to limit the extent to which a uniform text, once incorporated in local legislation, would be interpreted only by reference to the concepts of local law.

42. The purpose of paragraph (1) is to draw the attention of courts and other national authorities to the fact that the provisions of the Model Law (or the provisions of the instrument implementing the Model Law), while enacted as part of domestic legislation and therefore domestic in character, should be interpreted with reference to its international origin in order to ensure uniformity in the interpretation of the Model Law in various countries.

43. As to the general principles on which the Model Law is based, the following non-exhaustive list may be considered: (1) to facilitate electronic commerce among and within nations; (2) to validate transactions entered into by means of new information technologies; (3) to promote and encourage the implementation of new information technologies; (4) to promote the uniformity of law; and (5) to support commercial practice. While the general purpose of the Model Law is to facilitate the use of electronic means of communication, it should not be construed in any way as imposing their use.

*References*

A/50/17, paras. 220–224;
A/CN.9/407, paras. 53–54;
A/CN.9/406, paras. 86–87; A/CN.9/WG.IV/WP.62, article 3;
A/CN.9/390, paras. 66–73; A/CN.9/WG.IV/WP.60, article 3;
A/CN.9/387, paras. 53–58; A/CN.9/WG.IV/WP.57, article 3;
A/CN.9/373, paras. 38–42; A/CN.9/WG.IV/WP.55, paras. 30–31.

*Article 4. Variation by agreement*

44. The decision to undertake the preparation of the Model Law was based on the recognition that, in practice, solutions to the legal difficulties raised by the use of modern means of communication are mostly sought within contracts. The Model Law is thus intended to support the principle of party autonomy. However, that principle is embodied only with respect to the provisions of the Model Law contained in chapter III of part one. The reason for such a limitation is that the provisions contained in chapter II of part one may, to some extent, be regarded as a

collection of exceptions to well-established rules regarding the form of legal transactions. Such well-established rules are normally of a mandatory nature since they generally reflect decisions of public policy. An unqualified statement regarding the freedom of parties to derogate from the Model Law might thus be misinterpreted as allowing parties, through a derogation to the Model Law, to derogate from mandatory rules adopted for reasons of public policy. The provisions contained in chapter II of part one should be regarded as stating the minimum acceptable form requirement and are, for that reason, to be regarded as mandatory, unless expressly stated otherwise. The indication that such form requirements are to be regarded as the "minimum acceptable" should not, however, be construed as inviting States to establish requirements stricter than those contained in the Model Law.

45. Article 4 is intended to apply not only in the context of relationships between originators and addressees of data messages but also in the context of relationships involving intermediaries. Thus, the provisions of chapter III of part one could be varied either by bilateral or multilateral agreements between the parties, or by system rules agreed to by the parties. However, the text expressly limits party autonomy to rights and obligations arising as between parties so as not to suggest any implication as to the rights and obligations of third parties.

*References*

A/51/17, paras. 68, 90 to 93, 110, 137, 188 and 207 (article 10);
A/50/17, paras. 271–274 (article 10);
A/CN.9/407, para. 85;
A/CN.9/406, paras. 88–89; A/CN.9/WG.IV/WP.62, article 5;
A/CN.9/390, paras. 74–78; A/CN.9/WG.IV/WP.60, article 5;
A/CN.9/387, paras. 62–65; A/CN.9/WG.IV/WP.57, article 5;
A/CN.9/373, para. 37; A/CN.9/WG.IV/WP.55, paras. 27–29.

## Chapter II. Application of legal requirements to data messages

### *Article 5. Legal recognition of data messages*

46. Article 5 embodies the fundamental principle that data messages should not be discriminated against, i.e., that there should be no disparity of treatment between data messages and paper documents. It is intended to apply notwithstanding any statutory requirements for a "writing" or an original. That fundamental principle is intended to find general application and its scope should not be limited to evidence or other matters covered in chapter II. It should be noted, however, that such a principle is

not intended to override any of the requirements contained in articles 6 to 10. By stating that "information shall not be denied legal effectiveness, validity or enforceability solely on the grounds that it is in the form of a data message", article 5 merely indicates that the form in which certain information is presented or retained cannot be used as the only reason for which that information would be denied legal effectiveness, validity or enforceability. However, article 5 should not be misinterpreted as establishing the legal validity of any given data message or of any information contained therein.

*References*

A/51/17, paras. 92 and 97 (article 4); A/50/17, paras. 225–227 (article 4); A/CN.9/407, para. 55; A/CN.9/406, paras. 91–94; A/CN.9/WG.IV/WP. 62, article 5 bis; A/CN.9/390, paras. 79–87; A/CN.9/WG.IV/WP. 60, article 5 bis; A/CN.9/387, paras. 93–94.

*Article 5 bis. Incorporation by reference*

46-1. Article 5 bis was adopted by the Commission at its thirty-first session, in June 1998. It is intended to provide guidance as to how legislation aimed at facilitating the use of electronic commerce might deal with the situation where certain terms and conditions, although not stated in full but merely referred to in a data message, might need to be recognized as having the same degree of legal effectiveness as if they had been fully stated in the text of that data message. Such recognition is acceptable under the laws of many States with respect to conventional paper communications, usually with some rules of law providing safeguards, for example rules on consumer protection. The expression "incorporation by reference" is often used as a concise means of describing situations where a document refers generically to provisions which are detailed elsewhere, rather than reproducing them in full.

46-2. In an electronic environment, incorporation by reference is often regarded as essential to widespread use of electronic data interchange (EDI), electronic mail, digital certificates and other forms of electronic commerce. For example, electronic communications are typically structured in such a way that large numbers of messages are exchanged, with each message containing brief information, and relying much more frequently than paper documents on reference to information accessible elsewhere. In electronic communications, practitioners should not have imposed upon them an obligation to overload their data messages with quantities of free text when they can take advantage of extrinsic sources of information, such as databases, code lists or glossaries, by making use of abbreviations, codes and other references to such information.

46-3. Standards for incorporating data messages by reference into other data messages may also be essential to the use of public key certificates, because these certificates are generally brief records with rigidly prescribed contents that are finite in size. The trusted third party which issues the certificate, however, is likely to require the inclusion of relevant contractual terms limiting its liability. The scope, purpose and effect of a certificate in commercial practice, therefore, would be ambiguous and uncertain without external terms being incorporated by reference. This is the case especially in the context of international communications involving diverse parties who follow varied trade practices and customs.

46-4. The establishment of standards for incorporating data messages by reference into other data messages is critical to the growth of a computer-based trade infrastructure. Without the legal certainty fostered by such standards, there might be a significant risk that the application of traditional tests for determining the enforceability of terms that seek to be incorporated by reference might be ineffective when applied to corresponding electronic commerce terms because of the differences between traditional and electronic commerce mechanisms.

46-5. While electronic commerce relies heavily on the mechanism of incorporation by reference, the accessibility of the full text of the information being referred to may be considerably improved by the use of electronic communications. For example, a message may have embedded in it uniform resource locators (URLs), which direct the reader to the referenced document. Such URLs can provide "hypertext links" allowing the reader to use a pointing device (such as a mouse) to select a key word associated with a URL. The referenced text would then be displayed. In assessing the accessibility of the referenced text, factors to be considered may include: availability (hours of operation of the repository and ease of access); cost of access; integrity (verification of content, authentication of sender, and mechanism for communication error correction); and the extent to which that term is subject to later amendment (notice of updates; notice of policy of amendment).

46-6. One aim of article 5 bis is to facilitate incorporation by reference in an electronic context by removing the uncertainty prevailing in many jurisdictions as to whether the provisions dealing with traditional incorporation by reference are applicable to incorporation by reference in an electronic environment. However, in enacting article 5 bis, attention should be given to avoid introducing more restrictive requirements with respect to

incorporation by reference in electronic commerce than might already apply in paper-based trade.

46-7. Another aim of the provision is to recognize that consumer-protection or other national or international law of a mandatory nature (e.g., rules protecting weaker parties in the context of contracts of adhesion) should not be interfered with. That result could also be achieved by validating incorporation by reference in an electronic environment "to the extent permitted by law", or by listing the rules of law that remain unaffected by article 5 bis. Article 5 bis is not to be interpreted as creating a specific legal regime for incorporation by reference in an electronic environment. Rather, by establishing a principle of non-discrimination, it is to be construed as making the domestic rules applicable to incorporation by reference in a paper-based environment equally applicable to incorporation by reference for the purposes of electronic commerce. For example, in a number of jurisdictions, existing rules of mandatory law only validate incorporation by reference provided that the following three conditions are met: (a) the reference clause should be inserted in the data message; (b) the document being referred to, e.g., general terms and conditions, should actually be known to the party against whom the reference document might be relied upon; and (c) the reference document should be accepted, in addition to being known, by that party.

*References*

A/53/17, paras. 212–221;
A/CN.9/450;
A/CN.9/446, paras. 14–24;
A/CN.9/WG.IV/WP.74;
A/52/17, paras. 248–250;
A/CN.9/437, paras. 151–155;
A/CN.9/WG.IV/WP. 71, paras 77–93;
A/51/17, paras. 222–223;
A/CN.9/421, paras. 109 and 114;
A/CN.9/WG.IV/WP.69, paras. 30, 53, 59–60 and 91;
A/CN.9/407, paras. 100–105 and 117;
A/CN.9/WG.IV/WP.66;
A/CN.9/WG.IV/WP.65;
A/CN.9/406, paras. 90 and 178–179;
A/CN.9/WG.IV/WP.55, paras. 109–113;
A/CN.9/360, paras. 90–95;
A/CN.9/WG.IV/WP.53, paras. 77–78;
A/CN.9/350, paras. 95–96;
A/CN.9/333, paras. 66–68.

### *Article 6. Writing*

47. Article 6 is intended to define the basic standard to be met by a data message in order to be considered as meeting a requirement (which may result from statute, regulation or judge-made law) that information be retained or presented "in writing" (or that the information be contained in a "document" or other paper-based instrument). It may be noted that article 6 is part of a

set of three articles (articles 6, 7 and 8), which share the same structure and should be read together.

48. In the preparation of the Model Law, particular attention was paid to the functions traditionally performed by various kinds of "writings" in a paper-based environment. For example, the following non-exhaustive list indicates reasons why national laws require the use of "writings": (1) to ensure that there would be tangible evidence of the existence and nature of the intent of the parties to bind themselves; (2) to help the parties be aware of the consequences of their entering into a contract; (3) to provide that a document would be legible by all; (4) to provide that a document would remain unaltered over time and provide a permanent record of a transaction; (5) to allow for the reproduction of a document so that each party would hold a copy of the same data; (6) to allow for the authentication of data by means of a signature; (7) to provide that a document would be in a form acceptable to public authorities and courts; (8) to finalize the intent of the author of the "writing" and provide a record of that intent; (9) to allow for the easy storage of data in a tangible form; (10) to facilitate control and subsequent audit for accounting, tax or regulatory purposes; and (11) to bring legal rights and obligations into existence in those cases where a "writing" was required for validity purposes.

49. However, in the preparation of the Model Law, it was found that it would be inappropriate to adopt an overly comprehensive notion of the functions performed by writing. Existing requirements that data be presented in written form often combine the requirement of a "writing" with concepts distinct from writing, such as signature and original. Thus, when adopting a functional approach, attention should be given to the fact that the requirement of a "writing" should be considered as the lowest layer in a hierarchy of form requirements, which provide distinct levels of reliability, traceability and unalterability with respect to paper documents. The requirement that data be presented in written form (which can be described as a "threshold requirement") should thus not be confused with more stringent requirements such as "signed writing", "signed original" or "authenticated legal act". For example, under certain national laws, a written document that is neither dated nor signed, and the author of which either is not identified in the written document or is identified by a mere letterhead, would be regarded as a "writing" although it might be of little evidential weight in the absence of other evidence (e.g., testimony) regarding the authorship of the document. In addition, the notion of unalterability should not be considered as built into the concept of writing as an absolute requirement since a "writing"

in pencil might still be considered a "writing" under certain existing legal definitions. Taking into account the way in which such issues as integrity of the data and protection against fraud are dealt with in a paper-based environment, a fraudulent document would nonetheless be regarded as a "writing". In general, notions such as "evidence" and "intent of the parties to bind themselves" are to be tied to the more general issues of reliability and authentication of the data and should not be included in the definition of a "writing".

50. The purpose of article 6 is not to establish a requirement that, in all instances, data messages should fulfil all conceivable functions of a writing. Rather than focusing upon specific functions of a "writing", for example, its evidentiary function in the context of tax law or its warning function in the context of civil law, article 6 focuses upon the basic notion of the information being reproduced and read. That notion is expressed in article 6 in terms that were found to provide an objective criterion, namely that the information in a data message must be accessible so as to be usable for subsequent reference. The use of the word "accessible" is meant to imply that information in the form of computer data should be readable and interpretable, and that the software that might be necessary to render such information readable should be retained. The word "usable" is not intended to cover only human use but also computer processing. As to the notion of "subsequent reference", it was preferred to such notions as "durability" or "non-alterability", which would have established too harsh standards, and to such notions as "readability" or "intelligibility", which might constitute too subjective criteria.

51. The principle embodied in paragraph (3) of articles 6 and 7, and in paragraph (4) of article 8, is that an enacting State may exclude from the application of those articles certain situations to be specified in the legislation enacting the Model Law. An enacting State may wish to exclude specifically certain types of situations, depending in particular on the purpose of the formal requirement in question. One such type of situation may be the case of writing requirements intended to provide notice or warning of specific factual or legal risks, for example, requirements for warnings to be placed on certain types of products. Another specific exclusion might be considered, for example, in the context of formalities required pursuant to international treaty obligations of the enacting State (e.g., the requirement that a cheque be in writing pursuant to the Convention providing a Uniform Law for Cheques, Geneva, 1931) and other kinds of situations and areas of law that are beyond the power of the enacting State to change by means of a statute.

52. Paragraph (3) was included with a view to enhancing the acceptability of the Model Law. It recognizes that the matter of specifying exclusions should be left to enacting States, an approach that would take better account of differences in national circumstances. However, it should be noted that the objectives of the Model Law would not be achieved if paragraph (3) were used to establish blanket exceptions, and the opportunity provided by paragraph (3) in that respect should be avoided. Numerous exclusions from the scope of articles 6 to 8 would raise needless obstacles to the development of modern communication techniques, since what the Model Law contains are very fundamental principles and approaches that are expected to find general application.

*References*

A/51/17, paras. 180–181 and 185–187 (article 5);
A/50/17, paras. 228–241 (article 5);
A/CN.9/407, paras. 56–63;
A/CN.9/406, paras. 95–101; A/CN.9/WG.IV/WP.62, article 6;
A/CN.9/390, paras. 88–96; A/CN.9/WG.IV/WP.60, article 6;
A/CN.9/387, paras. 66–80; A/CN.9/WG.IV/WP.57, article 6;
A/CN.9/WG.IV/WP.58, annex;
A/CN.9/373, paras. 45–62; A/CN.9/WG.IV/WP.55, paras. 36–49;
A/CN.9/360, paras. 32–43; A/CN.9/WG.IV/WP.53, paras. 37–45;
A/CN.9/350, paras. 68–78;
A/CN.9/333, paras. 20–28;
A/CN.9/265, paras. 59–72.

### *Article 7. Signature*

53. Article 7 is based on the recognition of the functions of a signature in a paper-based environment. In the preparation of the Model Law, the following functions of a signature were considered: to identify a person; to provide certainty as to the personal involvement of that person in the act of signing; to associate that person with the content of a document. It was noted that, in addition, a signature could perform a variety of functions, depending on the nature of the document that was signed. For example, a signature might attest to the intent of a party to be bound by the content of a signed contract; the intent of a person to endorse authorship of a text; the intent of a person to associate itself with the content of a document written by someone else; the fact that, and the time when, a person had been at a given place.

54. It may be noted that, alongside the traditional handwritten signature, there exist various types of procedures (e.g., stamping, perforation), sometimes also referred to as "signatures", which provide various levels of certainty. For example, in some countries, there exists a general requirement that contracts for the sale of goods above a certain amount should be "signed" in order to be

enforceable. However, the concept of a signature adopted in that context is such that a stamp, perforation or even a typewritten signature or a printed letterhead might be regarded as sufficient to fulfil the signature requirement. At the other end of the spectrum, there exist requirements that combine the traditional handwritten signature with additional security procedures such as the confirmation of the signature by witnesses.

55. It might be desirable to develop functional equivalents for the various types and levels of signature requirements in existence. Such an approach would increase the level of certainty as to the degree of legal recognition that could be expected from the use of the various means of authentication used in electronic commerce practice as substitutes for "signatures". However, the notion of signature is intimately linked to the use of paper. Furthermore, any attempt to develop rules on standards and procedures to be used as substitutes for specific instances of "signatures" might create the risk of tying the legal framework provided by the Model Law to a given state of technical development.

56. With a view to ensuring that a message that was required to be authenticated should not be denied legal value for the sole reason that it was not authenticated in a manner peculiar to paper documents, article 7 adopts a comprehensive approach. It establishes the general conditions under which data messages would be regarded as authenticated with sufficient credibility and would be enforceable in the face of signature requirements which currently present barriers to electronic commerce. Article 7 focuses on the two basic functions of a signature, namely to identify the author of a document and to confirm that the author approved the content of that document. Paragraph (1)*(a)* establishes the principle that, in an electronic environment, the basic legal functions of a signature are performed by way of a method that identifies the originator of a data message and confirms that the originator approved the content of that data message.

57. Paragraph (1)*(b)* establishes a flexible approach to the level of security to be achieved by the method of identification used under paragraph (1)*(a)*. The method used under paragraph (1)*(a)* should be as reliable as is appropriate for the purpose for which the data message is generated or communicated, in the light of all the circumstances, including any agreement between the originator and the addressee of the data message.

58. In determining whether the method used under paragraph (1) is appropriate, legal, technical and commercial factors that may be taken into account include the following: (1) the

sophistication of the equipment used by each of the parties; (2) the nature of their trade activity; (3) the frequency at which commercial transactions take place between the parties; (4) the kind and size of the transaction; (5) the function of signature requirements in a given statutory and regulatory environment; (6) the capability of communication systems; (7) compliance with authentication procedures set forth by intermediaries; (8) the range of authentication procedures made available by any intermediary; (9) compliance with trade customs and practice; (10) the existence of insurance coverage mechanisms against unauthorized messages; (11) the importance and the value of the information contained in the data message; (12) the availability of alternative methods of identification and the cost of implementation; (13) the degree of acceptance or non-acceptance of the method of identification in the relevant industry or field both at the time the method was agreed upon and the time when the data message was communicated; and (14) any other relevant factor.

59. Article 7 does not introduce a distinction between the situation in which users of electronic commerce are linked by a communication agreement and the situation in which parties had no prior contractual relationship regarding the use of electronic commerce. Thus, article 7 may be regarded as establishing a basic standard of authentication for data messages that might be exchanged in the absence of a prior contractual relationship and, at the same time, to provide guidance as to what might constitute an appropriate substitute for a signature if the parties used electronic communications in the context of a communication agreement. The Model Law is thus intended to provide useful guidance both in a context where national laws would leave the question of authentication of data messages entirely to the discretion of the parties and in a context where requirements for signature, which were usually set by mandatory provisions of national law, should not be made subject to alteration by agreement of the parties.

60. The notion of an "agreement between the originator and the addressee of a data message" is to be interpreted as covering not only bilateral or multilateral agreements concluded between parties exchanging directly data messages (e.g., "trading partners agreements", "communication agreements" or " interchange agreements") but also agreements involving intermediaries such as networks (e.g., "third-party service agreements"). Agreements concluded between users of electronic commerce and networks may incorporate "system rules", i.e., administrative and technical rules and procedures to be applied when communicating data messages.

However, a possible agreement between originators and addressees of data messages as to the use of a method of authentication is not conclusive evidence of whether that method is reliable or not.

61. It should be noted that, under the Model Law, the mere signing of a data message by means of a functional equivalent of a handwritten signature is not intended, in and of itself, to confer legal validity on the data message. Whether a data message that fulfilled the requirement of a signature has legal validity is to be settled under the law applicable outside the Model Law.

*References*

A/51/17, paras. 180–181 and 185–187 (article 6);
A/50/17, paras. 242–248 (article 6);
A/CN.9/407, paras. 64–70;
A/CN.9/406, paras. 102–105; A/CN.9/WG.IV/WP.62, article 7;
A/CN.9/390, paras. 97–109; A/CN.9/WG.IV/WP.60, article 7;
A/CN.9/387, paras. 81–90; A/CN.9/WG.IV/WP.57, article 7; A/CN.9/WG.IV/WP.58, annex;
A/CN.9/373, paras. 63–76; A/CN.9/WG.IV/WP.55, paras. 50–63;
A/CN.9/360, paras. 71–75; A/CN.9/WG.IV/WP.53, paras. 61–66;
A/CN.9/350, paras. 86–89;
A/CN.9/333, paras. 50–59;
A/CN.9/265, paras. 49–58 and 79–80.

### *Article 8. Original*

62. If "original" were defined as a medium on which information was fixed for the first time, it would be impossible to speak of "original" data messages, since the addressee of a data message would always receive a copy thereof. However, article 8 should be put in a different context. The notion of "original" in article 8 is useful since in practice many disputes relate to the question of originality of documents, and in electronic commerce the requirement for presentation of originals constitutes one of the main obstacles that the Model Law attempts to remove. Although in some jurisdictions the concepts of "writing", "original" and "signature" may overlap, the Model Law approaches them as three separate and distinct concepts. Article 8 is also useful in clarifying the notions of "writing" and "original", in particular in view of their importance for purposes of evidence.

63. Article 8 is pertinent to documents of title and negotiable instruments, in which the notion of uniqueness of an original is particularly relevant. However, attention is drawn to the fact that the Model Law is not intended only to apply to documents of title and negotiable instruments, or to such areas of law where special requirements exist with respect to registration or notarization of "writings", e.g., family matters or the sale of real estate. Examples

of documents that might require an "original" are trade documents such as weight certificates, agricultural certificates, quality or quantity certificates, inspection reports, insurance certificates, etc. While such documents are not negotiable or used to transfer rights or title, it is essential that they be transmitted unchanged, that is in their "original" form, so that other parties in international commerce may have confidence in their contents. In a paper-based environment, these types of document are usually only accepted if they are "original" to lessen the chance that they be altered, which would be difficult to detect in copies. Various technical means are available to certify the contents of a data message to confirm its "originality". Without this functional equivalent of originality, the sale of goods using electronic commerce would be hampered since the issuers of such documents would be required to retransmit their data message each and every time the goods are sold, or the parties would be forced to use paper documents to supplement the electronic commerce transaction.

64. Article 8 should be regarded as stating the minimum acceptable form requirement to be met by a data message for it to be regarded as the functional equivalent of an original. The provisions of article 8 should be regarded as mandatory, to the same extent that existing provisions regarding the use of paper-based original documents would be regarded as mandatory. The indication that the form requirements stated in article 8 are to be regarded as the "minimum acceptable" should not, however, be construed as inviting States to establish requirements stricter than those contained in the Model Law.

65. Article 8 emphasizes the importance of the integrity of the information for its originality and sets out criteria to be taken into account when assessing integrity by reference to systematic recording of the information, assurance that the information was recorded without lacunae and protection of the data against alteration. It links the concept of originality to a method of authentication and puts the focus on the method of authentication to be followed in order to meet the requirement. It is based on the following elements: a simple criterion as to "integrity" of the data; a description of the elements to be taken into account in assessing the integrity; and an element of flexibility, i.e., a reference to circumstances.

66. As regards the words "the time when it was first generated in its final form" in paragraph (1)(*a*), it should be noted that the provision is intended to encompass the situation where information

was first composed as a paper document and subsequently transferred on to a computer. In such a situation, paragraph (1)*(a)* is to be interpreted as requiring assurances that the information has remained complete and unaltered from the time when it was composed as a paper document onwards, and not only as from the time when it was translated into electronic form. However, where several drafts were created and stored before the final message was composed, paragraph (1)*(a)* should not be misinterpreted as requiring assurance as to the integrity of the drafts.

67. Paragraph (3)*(a)* sets forth the criteria for assessing integrity, taking care to except necessary additions to the first (or "original") data message such as endorsements, certifications, notarizations, etc. from other alterations. As long as the contents of a data message remain complete and unaltered, necessary additions to that data message would not affect its "originality". Thus when an electronic certificate is added to the end of an "original" data message to attest to the "originality" of that data message, or when data is automatically added by computer systems at the start and the finish of a data message in order to transmit it, such additions would be considered as if they were a supplemental piece of paper with an "original" piece of paper, or the envelope and stamp used to send that "original" piece of paper.

68. As in other articles of chapter II of part one, the words "the law" in the opening phrase of article 8 are to be understood as encompassing not only statutory or regulatory law but also judicially-created law and other procedural law. In certain common law countries, where the words "the law" would normally be interpreted as referring to common law rules, as opposed to statutory requirements, it should be noted that, in the context of the Model Law, the words "the law" are intended to encompass those various sources of law. However, "the law", as used in the Model Law, is not meant to include areas of law that have not become part of the law of a State and are sometimes, somewhat imprecisely, referred to by expressions such as "*lex mercatoria*" or "law merchant".

69. Paragraph (4), as was the case with similar provisions in articles 6 and 7, was included with a view to enhancing the acceptability of the Model Law. It recognizes that the matter of specifying exclusions should be left to enacting States, an approach that would take better account of differences in national circumstances. However, it should be noted that the objectives of the Model Law would not be achieved if paragraph (4) were used

to establish blanket exceptions. Numerous exclusions from the scope of articles 6 to 8 would raise needless obstacles to the development of modern communication techniques, since what the Model Law contains are very fundamental principles and approaches that are expected to find general application.

*References*

A/51/17, paras. 180–181 and 185–187 (article 7);
A/50/17, paras. 249–255 (article 7);
A/CN.9/407, paras. 71–79;
A/CN.9/406, paras. 106–110; A/CN.9/WG.IV/WP.62, article 8;
A/CN.9/390, paras. 110–133; A/CN.9/WG.IV/WP.60, article 8;
A/CN.9/387, paras. 91–97; A/CN.9/WG.IV/WP.57, article 8;
A/CN.9/WG.IV/WP.58, annex;
A/CN.9/373, paras. 77–96;
A/CN.9/WG.IV/WP.55, paras. 64–70;
A/CN.9/360, paras. 60–70; A/CN.9/WG.IV/WP.53, paras. 56–60;
A/CN.9/350, paras. 84–85;
A/CN.9/265, paras. 43–48.

*Article 9. Admissibility and evidential weight of data messages*

70. The purpose of article 9 is to establish both the admissibility of data messages as evidence in legal proceedings and their evidential value. With respect to admissibility, paragraph (1), establishing that data messages should not be denied admissibility as evidence in legal proceedings on the sole ground that they are in electronic form, puts emphasis on the general principle stated in article 4 and is needed to make it expressly applicable to admissibility of evidence, an area in which particularly complex issues might arise in certain jurisdictions. The term "best evidence" is a term understood in, and necessary for, certain common law jurisdictions. However, the notion of "best evidence" could raise a great deal of uncertainty in legal systems in which such a rule is unknown. States in which the term would be regarded as meaningless and potentially misleading may wish to enact the Model Law without the reference to the "best evidence" rule contained in paragraph (1).

71. As regards the assessment of the evidential weight of a data message, paragraph (2) provides useful guidance as to how the evidential value of data messages should be assessed (e.g., depending on whether they were generated, stored or communicated in a reliable manner).

*References*

A/50/17, paras. 256–263 (article 8);
A/CN.9/407, paras. 80–81;
A/CN.9/406, paras. 111–113; A/CN.9/WG.IV/WP.62, article 9;
A/CN.9/390, paras. 139–143; A/CN.9/WG.IV/WP.60, article 9;
A/CN.9/387, paras. 98–109; A/CN.9/WG.IV/WP.57, article 9;
A/CN.9/WG.IV/WP.58, annex;

A/CN.9/373, paras. 97–108; A/CN.9/WG.IV/WP.55, paras. 71–81;
A/CN.9/360, paras. 44–59; A/CN.9/WG.IV/WP.53, paras. 46–55;
A/CN.9/350, paras. 79–83 and 90–91;
A/CN.9/333, paras. 29–41;
A/CN.9/265, paras. 27–48.

*Article 10. Retention of data messages*

72. Article 10 establishes a set of alternative rules for existing requirements regarding the storage of information (e.g., for accounting or tax purposes) that may constitute obstacles to the development of modern trade.

73. Paragraph (1) is intended to set out the conditions under which the obligation to store data messages that might exist under the applicable law would be met. Subparagraph *(a)* reproduces the conditions established under article 6 for a data message to satisfy a rule which prescribes the presentation of a "writing". Subparagraph *(b)* emphasizes that the message does not need to be retained unaltered as long as the information stored accurately reflects the data message as it was sent. It would not be appropriate to require that information should be stored unaltered, since usually messages are decoded, compressed or converted in order to be stored.

74. Subparagraph *(c)* is intended to cover all the information that may need to be stored, which includes, apart from the message itself, certain transmittal information that may be necessary for the identification of the message. Subparagraph *(c)*, by imposing the retention of the transmittal information associated with the data message, is creating a standard that is higher than most standards existing under national laws as to the storage of paper-based communications. However, it should not be understood as imposing an obligation to retain transmittal information additional to the information contained in the data message when it was generated, stored or transmitted, or information contained in a separate data message, such as an acknowledgement of receipt. Moreover, while some transmittal information is important and has to be stored, other transmittal information can be exempted without the integrity of the data message being compromised. That is the reason why subparagraph *(c)* establishes a distinction between those elements of transmittal information that are important for the identification of the message and the very few elements of transmittal information covered in paragraph (2) (e.g., communication protocols), which are of no value with regard to the data message and which, typically, would automatically be

stripped out of an incoming data message by the receiving computer before the data message actually entered the information system of the addressee.

75. In practice, storage of information, and especially storage of transmittal information, may often be carried out by someone other than the originator or the addressee, such as an intermediary. Nevertheless, it is intended that the person obligated to retain certain transmittal information cannot escape meeting that obligation simply because, for example, the communications system operated by that other person does not retain the required information. This is intended to discourage bad practice or wilful misconduct. Paragraph (3) provides that in meeting its obligations under paragraph (1), an addressee or originator may use the services of any third party, not just an intermediary.

*References*

A/51/17, paras. 185–187 (article 9);
A/50/17, paras. 264–270 (article 9);
A/CN.9/407, paras. 82–84;
A/CN.9/406, paras. 59–72; A/CN.9/WG.IV/WP.60, article 14;
A/CN.9/387, paras. 164–168;
A/CN.9/WG.IV/WP.57, article 14;
A/CN.9/373, paras. 123–125;
A/CN.9/WG.IV/WP.55, para. 94.

## Chapter III. Communication of data messages

### *Article 11. Formation and validity of contracts*

76. Article 11 is not intended to interfere with the law on formation of contracts but rather to promote international trade by providing increased legal certainty as to the conclusion of contracts by electronic means. It deals not only with the issue of contract formation but also with the form in which an offer and an acceptance may be expressed. In certain countries, a provision along the lines of paragraph (1) might be regarded as merely stating the obvious, namely that an offer and an acceptance, as any other expression of will, can be communicated by any means, including data messages. However, the provision is needed in view of the remaining uncertainties in a considerable number of countries as to whether contracts can validly be concluded by electronic means. Such uncertainties may stem from the fact that, in certain cases, the data messages expressing offer and acceptance are generated by computers without immediate human intervention, thus raising doubts as to the expression of intent by the parties. Another reason for such uncertainties is inherent in the mode of communication and results from the absence of a paper document.

77. It may also be noted that paragraph (1) reinforces, in the context of contract formation, a principle already embodied in other articles of the Model Law, such as articles 5, 9 and 13, all of which establish the legal effectiveness of data messages. However, paragraph (1) is needed since the fact that electronic messages may have legal value as evidence and produce a number of effects, including those provided in articles 9 and 13, does not necessarily mean that they can be used for the purpose of concluding valid contracts.

78. Paragraph (1) covers not merely the cases in which both the offer and the acceptance are communicated by electronic means but also cases in which only the offer or only the acceptance is communicated electronically. As to the time and place of formation of contracts in cases where an offer or the acceptance of an offer is expressed by means of a data message, no specific rule has been included in the Model Law in order not to interfere with national law applicable to contract formation. It was felt that such a provision might exceed the aim of the Model Law, which should be limited to providing that electronic communications would achieve the same degree of legal certainty as paper-based communications. The combination of existing rules on the formation of contracts with the provisions contained in article 15 is designed to dispel uncertainty as to the time and place of formation of contracts in cases where the offer or the acceptance are exchanged electronically.

79. The words "unless otherwise stated by the parties", which merely restate, in the context of contract formation, the recognition of party autonomy expressed in article 4, are intended to make it clear that the purpose of the Model Law is not to impose the use of electronic means of communication on parties who rely on the use of paper-based communication to conclude contracts. Thus, article 11 should not be interpreted as restricting in any way party autonomy with respect to parties not involved in the use of electronic communication.

80. During the preparation of paragraph (1), it was felt that the provision might have the harmful effect of overruling otherwise applicable provisions of national law, which might prescribe specific formalities for the formation of certain contracts. Such forms include notarization and other requirements for "writings", and might respond to considerations of public policy, such as the need to protect certain parties or to warn them against specific risks. For that reason, paragraph (2) provides that an enacting State

can exclude the application of paragraph (1) in certain instances to be specified in the legislation enacting the Model Law.

*References*

A/51/17, paras. 89–94 (article 13);
A/CN.9/407, para. 93;
A/CN.9/406, paras. 34–41; A/CN.9/WG.IV/WP.60, article 12;
A/CN.9/387, paras. 145–151; A/CN.9/WG.IV/WP.57, article 12;
A/CN.9/373, paras. 126–133; A/CN.9/WG.IV/WP.55, paras. 95–102;
A/CN.9/360, paras. 76–86; A/CN.9/WG.IV/WP.53, paras. 67–73;
A/CN.9/350, paras. 93–96;
A/CN.9/333, paras. 60–68.

### *Article 12. Recognition by parties of data messages*

81. Article 12 was added at a late stage in the preparation of the Model Law, in recognition of the fact that article 11 was limited to dealing with data messages that were geared to the conclusion of a contract, but that the draft Model Law did not contain specific provisions on data messages that related not to the conclusion of contracts but to the performance of contractual obligations (e.g., notice of defective goods, an offer to pay, notice of place where a contract would be performed, recognition of debt). Since modern means of communication are used in a context of legal uncertainty, in the absence of specific legislation in most countries, it was felt appropriate for the Model Law not only to establish the general principle that the use of electronic communication should not be discriminated against, as expressed in article 5, but also to include specific illustrations of that principle. Contract formation is but one of the areas where such an illustration is useful and the legal validity of unilateral expressions of will, as well as other notices or statements that may be issued in the form of data messages, also needs to be mentioned.

82. As is the case with article 11, article 12 is not to impose the use of electronic means of communication but to validate such use, subject to contrary agreement by the parties. Thus, article 12 should not be used as a basis to impose on the addressee the legal consequences of a message, if the use of a non-paper-based method for its transmission comes as a surprise to the addressee.

*References*

A/51/17, paras. 95–99 (new article 13 bis).

### *Article 13. Attribution of data messages*

83. Article 13 has its origin in article 5 of the UNCITRAL Model Law on International Credit Transfers, which defines the obligations of the sender of a payment order. Article 13 is intended to apply where there is a question as to whether a data message

was really sent by the person who is indicated as being the originator. In the case of a paper-based communication the problem would arise as the result of an alleged forged signature of the purported originator. In an electronic environment, an unauthorized person may have sent the message but the authentication by code, encryption or the like would be accurate. The purpose of article 13 is not to assign responsibility. It deals rather with attribution of data messages by establishing a presumption that under certain circumstances a data message would be considered as a message of the originator, and goes on to qualify that presumption in case the addressee knew or ought to have known that the data message was not that of the originator.

84. Paragraph (1) recalls the principle that an originator is bound by a data message if it has effectively sent that message. Paragraph (2) refers to the situation where the message was sent by a person other than the originator who had the authority to act on behalf of the originator. Paragraph (2) is not intended to displace the domestic law of agency, and the question as to whether the other person did in fact and in law have the authority to act on behalf of the originator is left to the appropriate legal rules outside the Model Law.

85. Paragraph (3) deals with two kinds of situations, in which the addressee could rely on a data message as being that of the originator: firstly, situations in which the addressee properly applied an authentication procedure previously agreed to by the originator; and secondly, situations in which the data message resulted from the actions of a person who, by virtue of its relationship with the originator, had access to the originator's authentication procedures. By stating that the addressee "is entitled to regard a data as being that of the originator", paragraph (3) read in conjunction with paragraph (4)*(a)* is intended to indicate that the addressee could act on the assumption that the data message is that of the originator up to the point in time it received notice from the originator that the data message was not that of the originator, or up to the point in time when it knew or should have known that the data message was not that of the originator.

86. Under paragraph (3)*(a)*, if the addressee applies any authentication procedures previously agreed to by the originator and such application results in the proper verification of the originator as the source of the message, the message is presumed to be that of the originator. That covers not only the situation where an authentication procedure has been agreed upon by the originator and the addressee but also situations where an originator,

unilaterally or as a result of an agreement with an intermediary, identified a procedure and agreed to be bound by a data message that met the requirements corresponding to that procedure. Thus, agreements that became effective not through direct agreement between the originator and the addressee but through the participation of third-party service providers are intended to be covered by paragraph (3)*(a)*. However, it should be noted that paragraph (3)*(a)* applies only when the communication between the originator and the addressee is based on a previous agreement, but that it does not apply in an open environment.

87. The effect of paragraph (3)*(b)*, read in conjunction with paragraph (4)*(b)*, is that the originator or the addressee, as the case may be, is responsible for any unauthorized data message that can be shown to have been sent as a result of negligence of that party.

88. Paragraph (4)*(a)* should not be misinterpreted as relieving the originator from the consequences of sending a data message, with retroactive effect, irrespective of whether the addressee had acted on the assumption that the data message was that of the originator. Paragraph (4) is not intended to provide that receipt of a notice under subparagraph *(a)* would nullify the original message retroactively. Under subparagraph *(a)*, the originator is released from the binding effect of the message after the time notice is received and not before that time. Moreover, paragraph (4) should not be read as allowing the originator to avoid being bound by the data message by sending notice to the addressee under subparagraph *(a)*, in a case where the message had, in fact, been sent by the originator and the addressee properly applied agreed or reasonable authentication procedures. If the addressee can prove that the message is that of the originator, paragraph (1) would apply and not paragraph (4)*(a)*. As to the meaning of "reasonable time", the notice should be such as to give the addressee sufficient time to react. For example, in the case of just-in-time supply, the addressee should be given time to adjust its production chain.

89. With respect to paragraph (4)*(b)*, it should be noted that the Model Law could lead to the result that the addressee would be entitled to rely on a data message under paragraph (3)*(a)* if it had properly applied the agreed authentication procedures, even if it knew that the data message was not that of the originator. It was generally felt when preparing the Model Law that the risk that such a situation could arise should be accepted, in view of the need for preserving the reliability of agreed authentication procedures.

90. Paragraph (5) is intended to preclude the originator from disavowing the message once it was sent, unless the addressee knew, or should have known, that the data message was not that of the originator. In addition, paragraph (5) is intended to deal with errors in the content of the message arising from errors in transmission.

91. Paragraph (6) deals with the issue of erroneous duplication of data messages, an issue of considerable practical importance. It establishes the standard of care to be applied by the addressee to distinguish an erroneous duplicate of a data message from a separate data message.

92. Early drafts of article 13 contained an additional paragraph, expressing the principle that the attribution of authorship of a data message to the originator should not interfere with the legal consequences of that message, which should be determined by other applicable rules of national law. It was later felt that it was not necessary to express that principle in the Model Law but that it should be mentioned in this Guide.

*References*

A/51/17, paras. 189–194 (article 11);
A/50/17, paras. 275–303 (article 11);
A/CN.9/407, paras. 86–89;
A/CN.9/406, paras. 114–131; A/CN.9/WG.IV/WP.62, article 10;
A/CN.9/390, paras. 144–153; A/CN.9/WG.IV/WP.60, article 10;
A/CN.9/387, paras. 110–132; A/CN.9/WG.IV/WP.57, article 10;
A/CN.9/373, paras. 109–115; A/CN.9/WG.IV/WP.55, paras. 82–86.

### *Article 14. Acknowledgement of receipt*

93. The use of functional acknowledgements is a business decision to be made by users of electronic commerce; the Model Law does not intend to impose the use of any such procedure. However, taking into account the commercial value of a system of acknowledgement of receipt and the widespread use of such systems in the context of electronic commerce, it was felt that the Model Law should address a number of legal issues arising from the use of acknowledgement procedures. It should be noted that the notion of "acknowledgement" is sometimes used to cover a variety of procedures, ranging from a mere acknowledgement of receipt of an unspecified message to an expression of agreement with the content of a specific data message. In many instances, the procedure of "acknowledgement" would parallel the system known as "return receipt requested" in postal systems. Acknowledgements of receipt may be required in a variety of instruments, e.g., in the data message

itself, in bilateral or multilateral communication agreements, or in "system rules". It should be borne in mind that variety among acknowledgement procedures implies variety of the related costs. The provisions of article 14 are based on the assumption that acknowledgement procedures are to be used at the discretion of the originator. Article 14 is not intended to deal with the legal consequences that may flow from sending an acknowledgement of receipt, apart from establishing receipt of the data message. For example, where an originator sends an offer in a data message and requests acknowledgement of receipt, the acknowledgement of receipt simply evidences that the offer has been received. Whether or not sending that acknowledgement amounted to accepting the offer is not dealt with by the Model Law but by contract law outside the Model Law.

94. The purpose of paragraph (2) is to validate acknowledgement by any communication or conduct of the addressee (e.g., the shipment of the goods as an acknowledgement of receipt of a purchase order) where the originator has not agreed with the addressee that the acknowledgement should be in a particular form. The situation where an acknowledgement has been unilaterally requested by the originator to be given in a specific form is not expressly addressed by article 14, which may entail as a possible consequence that a unilateral requirement by the originator as to the form of acknowledgements would not affect the right of the addressee to acknowledge receipt by any communication or conduct sufficient to indicate to the originator that the message had been received. Such a possible interpretation of paragraph (2) makes it particularly necessary to emphasize in the Model Law the distinction to be drawn between the effects of an acknowledgement of receipt of a data message and any communication in response to the content of that data message, a reason why paragraph (7) is needed.

95. Paragraph (3), which deals with the situation where the originator has stated that the data message is conditional on receipt of an acknowledgement, applies whether or not the originator has specified that the acknowledgement should be received by a certain time.

96. The purpose of paragraph (4) is to deal with the more common situation where an acknowledgement is requested, without any statement being made by the originator that the data message is of no effect until an acknowledgement has been received. Such a provision is needed to establish the point in time when the originator of a data message who has requested an

acknowledgement of receipt is relieved from any legal implication of sending that data message if the requested acknowledgement has not been received. An example of a factual situation where a provision along the lines of paragraph (4) would be particularly useful would be that the originator of an offer to contract who has not received the requested acknowledgement from the addressee of the offer may need to know the point in time after which it is free to transfer the offer to another party. It may be noted that the provision does not create any obligation binding on the originator, but merely establishes means by which the originator, if it so wishes, can clarify its status in cases where it has not received the requested acknowledgement. It may also be noted that the provision does not create any obligation binding on the addressee of the data message, who would, in most circumstances, be free to rely or not to rely on any given data message, provided that it would bear the risk of the data message being unreliable for lack of an acknowledgement of receipt. The addressee, however, is protected since the originator who does not receive a requested acknowledgement may not automatically treat the data message as though it had never been transmitted, without giving further notice to the addressee. The procedure described under paragraph (4) is purely at the discretion of the originator. For example, where the originator sent a data message which under the agreement between the parties had to be received by a certain time, and the originator requested an acknowledgement of receipt, the addressee could not deny the legal effectiveness of the message simply by withholding the requested acknowledgement.

97. The rebuttable presumption established in paragraph (5) is needed to create certainty and would be particularly useful in the context of electronic communication between parties that are not linked by a trading-partners agreement. The second sentence of paragraph (5) should be read in conjunction with paragraph (5) of article 13, which establishes the conditions under which, in case of an inconsistency between the text of the data message as sent and the text as received, the text as received prevails.

98. Paragraph (6) corresponds to a certain type of acknowledgement, for example, an EDIFACT message establishing that the data message received is syntactically correct, i.e., that it can be processed by the receiving computer. The reference to technical requirements, which is to be construed primarily as a reference to "data syntax" in the context of EDI communications, may be less relevant in the context of the use of other means of communication, such as telegram or telex. In addition to mere consistency with the rules of "data syntax", technical requirements

set forth in applicable standards may include, for example, the use of procedures verifying the integrity of the contents of data messages.

99. Paragraph (7) is intended to dispel uncertainties that might exist as to the legal effect of an acknowledgement of receipt. For example, paragraph (7) indicates that an acknowledgement of receipt should not be confused with any communication related to the contents of the acknowledged message.

*References*

A/51/17, paras. 63–88 (article 12);
A/CN.9/407, paras. 90–92;
A/CN.9/406, paras. 15–33; A/CN.9/WG.IV/WP.60, article 11;
A/CN.9/387, paras. 133–144; A/CN.9/WG.IV/WP.57, article 11;
A/CN.9/373, paras. 116–122; A/CN.9/WG.IV/WP.55, paras. 87–93;
A/CN.9/360, para. 125; A/CN.9/WG.IV/WP.53, paras. 80–81;
A/CN.9/350, para. 92;
A/CN.9/333, paras. 48–49.

*Article 15. Time and place of dispatch and receipt of data messages*

100. Article 15 results from the recognition that, for the operation of many existing rules of law, it is important to ascertain the time and place of receipt of information. The use of electronic communication techniques makes those difficult to ascertain. It is not uncommon for users of electronic commerce to communicate from one State to another without knowing the location of information systems through which communication is operated. In addition, the location of certain communication systems may change without either of the parties being aware of the change. The Model Law is thus intended to reflect the fact that the location of information systems is irrelevant and sets forth a more objective criterion, namely, the place of business of the parties. In that connection, it should be noted that article 15 is not intended to establish a conflict-of-laws rule.

101. Paragraph (1) defines the time of dispatch of a data message as the time when the data message enters an information system outside the control of the originator, which may be the information system of an intermediary or an information system of the addressee. The concept of "dispatch" refers to the commencement of the electronic transmission of the data message. Where "dispatch" already has an established meaning, article 15 is intended to supplement national rules on dispatch and not to displace them. If dispatch occurs when the data message reaches an information system of the addressee, dispatch under paragraph (1) and receipt under paragraph (2) are simultaneous, except where the data message is sent to an information system of the addressee

that is not the information system designated by the addressee under paragraph (2)*(a)*.

102. Paragraph (2), the purpose of which is to define the time of receipt of a data message, addresses the situation where the addressee unilaterally designates a specific information system for the receipt of a message (in which case the designated system may or may not be an information system of the addressee), and the data message reaches an information system of the addressee that is not the designated system. In such a situation, receipt is deemed to occur when the data message is retrieved by the addressee. By "designated information system", the Model Law is intended to cover a system that has been specifically designated by a party, for instance in the case where an offer expressly specifies the address to which acceptance should be sent. The mere indication of an electronic mail or telecopy address on a letterhead or other document should not be regarded as express designation of one or more information systems.

103. Attention is drawn to the notion of "entry" into an information system, which is used for both the definition of dispatch and that of receipt of a data message. A data message enters an information system at the time when it becomes available for processing within that information system. Whether a data message which enters an information system is intelligible or usable by the addressee is outside the purview of the Model Law. The Model Law does not intend to overrule provisions of national law under which receipt of a message may occur at the time when the message enters the sphere of the addressee, irrespective of whether the message is intelligible or usable by the addressee. Nor is the Model Law intended to run counter to trade usages, under which certain encoded messages are deemed to be received even before they are usable by, or intelligible for, the addressee. It was felt that the Model Law should not create a more stringent requirement than currently exists in a paper-based environment, where a message can be considered to be received even if it is not intelligible for the addressee or not intended to be intelligible to the addressee (e.g., where encrypted data is transmitted to a depository for the sole purpose of retention in the context of intellectual property rights protection).

104. A data message should not be considered to be dispatched if it merely reached the information system of the addressee but failed to enter it. It may be noted that the Model Law does not expressly address the question of possible malfunctioning of information systems as a basis for liability. In particular, where the information

system of the addressee does not function at all or functions improperly or, while functioning properly, cannot be entered into by the data message (e.g., in the case of a telecopier that is constantly occupied), dispatch under the Model Law does not occur. It was felt during the preparation of the Model Law that the addressee should not be placed under the burdensome obligation to maintain its information system functioning at all times by way of a general provision.

105. The purpose of paragraph (4) is to deal with the place of receipt of a data message. The principal reason for including a rule on the place of receipt of a data message is to address a circumstance characteristic of electronic commerce that might not be treated adequately under existing law, namely, that very often the information system of the addressee where the data message is received, or from which the data message is retrieved, is located in a jurisdiction other than that in which the addressee itself is located. Thus, the rationale behind the provision is to ensure that the location of an information system is not the determinant element, and that there is some reasonable connection between the addressee and what is deemed to be the place of receipt, and that that place can be readily ascertained by the originator. The Model Law does not contain specific provisions as to how the designation of an information system should be made, or whether a change could be made after such a designation by the addressee.

106. Paragraph (4), which contains a reference to the "underlying transaction", is intended to refer to both actual and contemplated underlying transactions. References to "place of business", "principal place of business" and "place of habitual residence" were adopted to bring the text in line with article 10 of the United Nations Convention on Contracts for the International Sale of Goods.

107. The effect of paragraph (4) is to introduce a distinction between the deemed place of receipt and the place actually reached by a data message at the time of its receipt under paragraph (2). That distinction is not to be interpreted as apportioning risks between the originator and the addressee in case of damage or loss of a data message between the time of its receipt under paragraph (2) and the time when it reached its place of receipt under paragraph (4). Paragraph (4) merely establishes an irrebuttable presumption regarding a legal fact, to be used where another body of law (e.g., on formation of contracts or conflict of laws) require determination of the place of receipt of a data message. However, it was felt during the preparation of the Model Law that introducing

a deemed place of receipt, as distinct from the place actually reached by that data message at the time of its receipt, would be inappropriate outside the context of computerized transmissions (e.g., in the context of telegram or telex). The provision was thus limited in scope to cover only computerized transmissions of data messages. A further limitation is contained in paragraph (5), which reproduces a provision already included in articles 6, 7, 8, 11 and 12 (see above, para. 69).

*References*

A/51/17, paras. 100–115 (article 14);
A/CN.9/407, paras. 94–99;
A/CN.9/406, paras. 42–58; A/CN.9/WG.IV/WP.60, article 13;
A/CN.9/387, paras. 152–163; A/CN.9/WG.IV/WP.57, article 13;
A/CN.9/373, paras. 134–146; A/CN.9/WG.IV/WP.55, paras. 103–108;
A/CN.9/360, paras. 87–89; A/CN.9/WG.IV/WP.53, paras. 74–76;
A/CN.9/350, paras. 97–100;
A/CN.9/333, paras. 69–75.

## Part two. Electronic commerce in specific areas

108. As distinct from the basic rules applicable to electronic commerce in general, which appear as part one of the Model Law, part two contains rules of a more specific nature. In preparing the Model Law, the Commission agreed that such rules dealing with specific uses of electronic commerce should appear in the Model Law in a way that reflected both the specific nature of the provisions and their legal status, which should be the same as that of the general provisions contained in part one of the Model Law. While the Commission, when adopting the Model Law, only considered such specific provisions in the context of transport documents, it was agreed that such provisions should appear as chapter I of part two of the Model Law. It was felt that adopting such an open-ended structure would make it easier to add further specific provisions to the Model Law, as the need might arise, in the form of additional chapters in part two.

109. The adoption of a specific set of rules dealing with specific uses of electronic commerce, such as the use of EDI messages as substitutes for transport documents does not imply that the other provisions of the Model Law are not applicable to such documents. In particular, the provisions of part two, such as articles 16 and 17 concerning transfer of rights in goods, presuppose that the guarantees of reliability and authenticity contained in articles 6 to 8 of the Model Law are also applicable to electronic equivalents to transport documents. Part two of the Model Law does not in any way limit or restrict the field of application of the general provisions of the Model Law.

110. In preparing the Model Law, the Commission noted that the carriage of goods was the context in which electronic communications were most likely to be used and in which a legal framework facilitating the use of such communications was most urgently needed. Articles 16 and 17 contain provisions that apply equally to non-negotiable transport documents and to transfer of rights in goods by way of transferable bills of lading. The principles embodied in articles 16 and 17 are applicable not only to maritime transport but also to transport of goods by other means, such as road, railroad and air transport.

*Article 16. Actions related to contracts of carriage of goods*

111. Article 16, which establishes the scope of chapter I of part two of the Model Law, is broadly drafted. It would encompass a wide variety of documents used in the context of the carriage of goods, including, for example, charter-parties. In the preparation of the Model Law, the Commission found that, by dealing comprehensively with contracts of carriage of goods, article 16 was consistent with the need to cover all transport documents, whether negotiable or non-negotiable, without excluding any specific document such as charter-parties. It was pointed out that, if an enacting State did not wish chapter I of part two to apply to a particular kind of document or contract, for example if the inclusion of such documents as charter-parties in the scope of that chapter was regarded as inappropriate under the legislation of an enacting State, that State could make use of the exclusion clause contained in paragraph (7) of article 17.

112. Article 16 is of an illustrative nature and, although the actions mentioned therein are more common in maritime trade, they are not exclusive to such type of trade and could be performed in connection with air transport or multimodal carriage of goods.

*References*

A/51/17, paras. 139–172 and 198–204 (draft article x); A/CN.9/421, paras. 53–103; A/CN.9/WG.IV/WP.69, paras. 82–95; A/50/17, paras. 307–309; A/CN.9/407, paras. 106–118; A/CN.9/WG.IV/WP.67, annex; A/CN.9/WG.IV/WP.66, annex II; A/49/17, paras. 198, 199 and 201; A/CN.9/390, para. 155–158.

*Article 17. Transport documents*

113. Paragraphs (1) and (2) are derived from article 6. In the context of transport documents, it is necessary to establish not only functional equivalents of written information about the

actions referred to in article 16, but also functional equivalents of the performance of such actions through the use of paper documents. Functional equivalents are particularly needed for the transfer of rights and obligations by transfer of written documents. For example, paragraphs (1) and (2) are intended to replace both the requirement for a written contract of carriage and the requirements for endorsement and transfer of possession of a bill of lading. It was felt in the preparation of the Model Law that the focus of the provision on the actions referred to in article 16 should be expressed clearly, particularly in view of the difficulties that might exist, in certain countries, for recognizing the transmission of a data message as functionally equivalent to the physical transfer of goods, or to the transfer of a document of title representing the goods.

114. The reference to "one or more data messages" in paragraphs (1), (3) and (6) is not intended to be interpreted differently from the reference to "a data message" in the other provisions of the Model Law, which should also be understood as covering equally the situation where only one data message is generated and the situation where more than one data message is generated as support of a given piece of information. A more detailed wording was adopted in article 17 merely to reflect the fact that, in the context of transfer of rights through data messages, some of the functions traditionally performed through the single transmission of a paper bill of lading would necessarily imply the transmission of more than one data message and that such a fact, in itself, should entail no negative consequence as to the acceptability of electronic commerce in that area.

115. Paragraph (3), in combination with paragraph (4), is intended to ensure that a right can be conveyed to one person only, and that it would not be possible for more than one person at any point in time to lay claim to it. The effect of the two paragraphs is to introduce a requirement which may be referred to as the "guarantee of singularity". If procedures are made available to enable a right or obligation to be conveyed by electronic methods instead of by using a paper document, it is necessary that the guarantee of singularity be one of the essential features of such procedures. Technical security devices providing such a guarantee of singularity would almost necessarily be built into any communication system offered to the trading communities and would need to demonstrate their reliability. However, there is also a need to overcome requirements of law that the guarantee of singularity be demonstrated, for example in the case where paper documents such as bills of lading are traditionally used. A provision along the lines

of paragraph (3) is thus necessary to permit the use of electronic communication instead of paper documents.

116. The words "one person and no other person" should not be interpreted as excluding situations where more than one person might jointly hold title to the goods. For example, the reference to "one person" is not intended to exclude joint ownership of rights in the goods or other rights embodied in a bill of lading.

117. The notion that a data message should be "unique" may need to be further clarified, since it may lend itself to misinterpretation. On the one hand, all data messages are necessarily unique, even if they duplicate an earlier data message, since each data message is sent at a different time from any earlier data message sent to the same person. If a data message is sent to a different person, it is even more obviously unique, even though it might be transferring the same right or obligation. Yet, all but the first transfer might be fraudulent. On the other hand, if "unique" is interpreted as referring to a data message of a unique kind, or a transfer of a unique kind, then in that sense no data message is unique, and no transfer by means of a data message is unique. Having considered the risk of such misinterpretation, the Commission decided to retain the reference to the concepts of uniqueness of the data message and uniqueness of the transfer for the purposes of article 17, in view of the fact that the notions of "uniqueness" or "singularity" of transport documents were not unknown to practitioners of transport law and users of transport documents. It was decided, however, that this Guide should clarify that the words "a reliable method is used to render such data message or messages unique" should be interpreted as referring to the use of a reliable method to secure that data messages purporting to convey any right or obligation of a person might not be used by, or on behalf of, that person inconsistently with any other data messages by which the right or obligation was conveyed by or on behalf of that person.

118. Paragraph (5) is a necessary complement to the guarantee of singularity contained in paragraph (3). The need for security is an overriding consideration and it is essential to ensure not only that a method is used that gives reasonable assurance that the same data message is not multiplied, but also that no two media can be simultaneously used for the same purpose. Paragraph (5) addresses the fundamental need to avoid the risk of duplicate transport documents. The use of multiple forms of communication for different purposes, e.g., paper-based communications for ancillary messages and electronic communications for bills of lading, does not pose a problem. However, it is essential for the operation of

any system relying on electronic equivalents of bills of lading to avoid the possibility that the same rights could at any given time be embodied both in data messages and in a paper document. Paragraph (5) also envisages the situation where a party having initially agreed to engage in electronic communications has to switch to paper communications where it later becomes unable to sustain electronic communications.

119. The reference to "terminating" the use of data messages is open to interpretation. In particular, the Model Law does not provide information as to who would effect the termination. Should an enacting State decide to provide additional information in that respect, it might wish to indicate, for example, that, since electronic commerce is usually based on the agreement of the parties, a decision to "drop down" to paper communications should also be subject to the agreement of all interested parties. Otherwise, the originator would be given the power to choose unilaterally the means of communication. Alternatively, an enacting State might wish to provide that, since paragraph (5) would have to be applied by the bearer of a bill of lading, it should be up to the bearer to decide whether it preferred to exercise its rights on the basis of a paper bill of lading or on the basis of the electronic equivalent of such a document, and to bear the costs for its decision.

220. Paragraph (5), while expressly dealing with the situation where the use of data messages is replaced by the use of a paper document, is not intended to exclude the reverse situation. The switch from data messages to a paper document should not affect any right that might exist to surrender the paper document to the issuer and start again using data messages.

121. The purpose of paragraph (6) is to deal directly with the application of certain laws to contracts for the carriage of goods by sea. For example, under the Hague and Hague-Visby Rules, a contract of carriage means a contract that is covered by a bill of lading. Use of a bill of lading or similar document of title results in the Hague and Hague-Visby Rules applying compulsorily to a contract of carriage. Those rules would not automatically apply to contracts effected by one or more data message. Thus, a provision such as paragraph (6) is needed to ensure that the application of those rules is not excluded by the mere fact that data messages are used instead of a bill of lading in paper form. While paragraph (1) ensures that data messages are effective means for carrying out any of the actions listed in article 16, that provision does not deal with the substantive rules of law that might apply to a contract contained in, or evidenced by, data messages.

122. As to the meaning of the phrase "that rule shall not be inapplicable" in paragraph (6), a simpler way of expressing the same idea might have been to provide that rules applicable to contracts of carriage evidenced by paper documents should also apply to contracts of carriage evidenced by data messages. However, given the broad scope of application of article 17, which covers not only bills of lading but also a variety of other transport documents, such a simplified provision might have had the undesirable effect of extending the applicability of rules such as the Hamburg Rules and the Hague-Visby Rules to contracts to which such rules were never intended to apply. The Commission felt that the adopted wording was more suited to overcome the obstacle resulting from the fact that the Hague-Visby Rules and other rules compulsorily applicable to bills of lading would not automatically apply to contracts of carriage evidenced by data messages, without inadvertently extending the application of such rules to other types of contracts.

*References*

A/51/17, paras. 139–172 and 198–204 (draft article x);
A/CN.9/421, paras. 53–103; A/CN.9/WG.IV/WP.69, paras 82–95;
A/50/17, paras. 307–309
A/CN.9/407, paras. 106–118 A/CN.9/WG.IV/WP.67, annex;
A/CN.9/WG.IV/WP.66, annex II;
A/49/17, paras. 198, 199 and 201;
A/CN.9/390, para. 155–158.

---

## III. HISTORY AND BACKGROUND OF THE MODEL LAW

123. The UNCITRAL Model Law on Electronic Commerce was adopted by the United Nations Commission on International Trade Law (UNCITRAL) in 1996 in furtherance of its mandate to promote the harmonization and unification of international trade law, so as to remove unnecessary obstacles to international trade caused by inadequacies and divergences in the law affecting trade. Over the past quarter of a century, UNCITRAL, whose membership consists of States from all regions and of all levels of economic development, has implemented its mandate by formulating international conventions (the United Nations Conventions on Contracts for the International Sale of Goods, on the Limitation Period in the International Sale of Goods, on the Carriage of Goods by Sea, 1978 ("Hamburg Rules"), on the Liability of Operators of Transport Terminals in International Trade, on International Bills of Exchange and International Promissory Notes, and on Independent Guarantees and Stand-by Letters of Credit), model laws (the UNCITRAL Model Laws on International Commercial

Arbitration, on International Credit Transfers and on Procurement of Goods, Construction and Services), the UNCITRAL Arbitration Rules, the UNCITRAL Conciliation Rules, and legal guides (on construction contracts, countertrade transactions and electronic funds transfers).

124. The Model Law was prepared in response to a major change in the means by which communications are made between parties using computerized or other modern techniques in doing business (sometimes referred to as "trading partners"). The Model Law is intended to serve as a model to countries for the evaluation and modernization of certain aspects of their laws and practices in the field of commercial relationships involving the use of computerized or other modern communication techniques, and for the establishment of relevant legislation where none presently exists. The text of the Model Law, as reproduced above, is set forth in annex I to the report of UNCITRAL on the work of its twenty-ninth session.[2]

125. The Commission, at its seventeenth session (1984), considered a report of the Secretary-General entitled "Legal aspects of automatic data processing" (A/CN.9/254), which identified several legal issues relating to the legal value of computer records, the requirement of a "writing", authentication, general conditions, liability and bills of lading. The Commission took note of a report of the Working Party on Facilitation of International Trade Procedures (WP.4), which is jointly sponsored by the Economic Commission for Europe and the United Nations Conference on Trade and Development, and is responsible for the development of UN/EDIFACT standard messages. That report suggested that, since the legal problems arising in this field were essentially those of international trade law, the Commission as the core legal body in the field of international trade law appeared to be the appropriate central forum to undertake and coordinate the necessary action.[3] The Commission decided to place the subject of the legal implications of automatic data processing to the flow of international trade on its programme of work as a priority item.[4]

---

2. *Official Records of the General Assembly, Fifty-first Session, Supplement No. 17* (A/51/17), Annex I.

3. "*Legal aspects of automatic trade data interchange*" (TRADE/WP.4/R.185/Rev.1). The report submitted to the Working Party is reproduced in A/CN.9/238, annex.

4. *Official Records of the General Assembly, Thirty-ninth Session, Supplement No. 17* (A/39/17), para. 136.

126. At its eighteenth session (1985), the Commission had before it a report by the Secretariat entitled "Legal value of computer records" (A/CN.9/265). That report came to the conclusion that, on a global level, there were fewer problems in the use of data stored in computers as evidence in litigation than might have been expected. It noted that a more serious legal obstacle to the use of computers and computer-to-computer telecommunications in international trade arose out of requirements that documents had to be signed or be in paper form. After discussion of the report, the Commission adopted the following recommendation, which expresses some of the principles on which the Model Law is based:

"*The United Nations Commission on International Trade Law,*

"*Noting* that the use of automatic data processing (ADP) is about to become firmly established throughout the world in many phases of domestic and international trade as well as in administrative services,

"*Noting also* that legal rules based upon pre-ADP paper-based means of documenting international trade may create an obstacle to such use of ADP in that they lead to legal insecurity or impede the efficient use of ADP where its use is otherwise justified,

"*Noting further* with appreciation the efforts of the Council of Europe, the Customs Co-operation Council and the United Nations Economic Commission for Europe to overcome obstacles to the use of ADP in international trade arising out of these legal rules,

"*Considering* at the same time that there is no need for a unification of the rules of evidence regarding the use of computer records in international trade, in view of the experience showing that substantial differences in the rules of evidence as they apply to the paper-based system of documentation have caused so far no noticeable harm to the development of international trade,

"*Considering also* that the developments in the use of ADP are creating a desirability in a number of legal systems for an adaptation of existing legal rules to these developments, having due regard, however, to the need to encourage the employment of such ADP means that would provide the same or greater reliability as paper-based documentation,

"1. *Recommends* to Governments:

"*(a)* to review the legal rules affecting the use of computer records as evidence in litigation in order to eliminate unnecessary obstacles to their admission, to be assured that the rules are consistent with developments in technology, and to provide appropriate means for a court to evaluate the credibility of the data contained in those records;

"*(b)* to review legal requirements that certain trade transactions or trade related documents be in writing, whether the written form is a condition to the enforceability or to the validity of the transaction or document, with a view to permitting, where appropriate, the transaction or document to be recorded and transmitted in computer-readable form;

"*(c)* to review legal requirements of a handwritten signature or other paper-based method of authentication on trade related documents with a view to permitting, where appropriate, the use of electronic means of authentication;

"*(d)* to review legal requirements that documents for submission to governments be in writing and manually signed with a view to permitting, where appropriate, such documents to be submitted in computer-readable form to those administrative services which have acquired the necessary equipment and established the necessary procedures;

"2. *Recommends* to international organizations elaborating legal texts related to trade to take account of the present Recommendation in adopting such texts and, where appropriate, to consider modifying existing legal texts in line with the present Recommendation."[5]

127. That recommendation (hereinafter referred to as the "1985 UNCITRAL Recommendation") was endorsed by the General Assembly in resolution 40/71, paragraph 5*(b)*, of 11 December 1985 as follows:

*"The General Assembly,*

". . . Calls upon Governments and international organizations to take action, where appropriate, in conformity with the Commission's recommendation so as to ensure legal security in the context of the widest possible use of automated data processing in international trade; ...".[6]

128. As was pointed out in several documents and meetings involving the international electronic commerce community, e.g. in meetings of WP. 4, there was a general feeling that, in spite of the efforts made through the 1985 UNCITRAL Recommendation, little progress had been made to achieve the removal of the mandatory requirements in national legislation regarding the use of paper and handwritten signatures. It has been suggested by the Norwegian Committee on Trade Procedures (NORPRO) in a letter to the Secretariat that "one reason for this could be that the 1985 UNCITRAL Recommendation advises on the need for legal update, but does not give any indication of how it could be done". In this vein, the Commission considered what follow-up action to the 1985 UNCITRAL Recommendation could usefully be taken so as to enhance the needed modernization of legislation. The decision by UNCITRAL to formulate model legislation on legal issues of electronic data interchange and related means of

---

5. *Official Records of the General Assembly, Fortieth Session, Supplement No. 17* (A/40/17), para. 360.

6. Resolution 40/71 was reproduced in *United Nations Commission on International Trade Law Yearbook*, 1985, vol. XVI, Part One, D. (United Nations publication, Sales No. E.87.V.4).

communication may be regarded as a consequence of the process that led to the adoption by the Commission of the 1985 UNCITRAL Recommendation.

129. At its twenty-first session (1988), the Commission considered a proposal to examine the need to provide for the legal principles that would apply to the formation of international commercial contracts by electronic means. It was noted that there existed no refined legal structure for the important and rapidly growing field of formation of contracts by electronic means and that future work in that area could help to fill a legal vacuum and to reduce uncertainties and difficulties encountered in practice. The Commission requested the Secretariat to prepare a preliminary study on the topic.[7]

130. At its twenty-third session (1990), the Commission had before it a report entitled "Preliminary study of legal issues related to the formation of contracts by electronic means" (A/CN.9/333). The report summarized work that had been undertaken in the European Communities and in the United States of America on the requirement of a "writing" as well as other issues that had been identified as arising in the formation of contracts by electronic means. The efforts to overcome some of those problems by the use of model communication agreements were also discussed.[8]

131. At its twenty-fourth session (1991), the Commission had before it a report entitled "Electronic Data Interchange" (A/CN.9/350). The report described the current activities in the various organizations involved in the legal issues of electronic data interchange (EDI) and analysed the contents of a number of standard interchange agreements already developed or then being developed. It pointed out that such documents varied considerably according to the various needs of the different categories of users they were intended to serve and that the variety of contractual arrangements had sometimes been described as hindering the development of a satisfactory legal framework for the business use of electronic commerce. It suggested that there was a need for a general framework that would identify the issues and provide a set of legal principles and basic legal rules governing communication through electronic commerce. It concluded that such a basic

---

7. *Official Records of the General Assembly, Forty-third Session, Supplement No. 17* (A/43/17), paras. 46 and 47, and ibid., *Forty-fourth Session, Supplement No. 17* (A/44/17), para. 289.

8. Ibid., *Forty-fifth Session, Supplement No. 17* (A/45/17), paras. 38 to 40.

framework could, to a certain extent, be created by contractual arrangements between parties to an electronic commerce relationship and that the existing contractual frameworks that were proposed to the community of users of electronic commerce were often incomplete, mutually incompatible, and inappropriate for international use since they relied to a large extent upon the structures of local law.

132. With a view to achieving the harmonization of basic rules for the promotion of electronic commerce in international trade, the report suggested that the Commission might wish to consider the desirability of preparing a standard communication agreement for use in international trade. It pointed out that work by the Commission in this field would be of particular importance since it would involve participation of all legal systems, including those of developing countries that were already or would soon be confronted with the issues of electronic commerce.

133. The Commission was agreed that the legal issues of electronic commerce would become increasingly important as the use of electronic commerce developed and that it should undertake work in that field. There was wide support for the suggestion that the Commission should undertake the preparation of a set of legal principles and basic legal rules governing communication through electronic commerce.[9] The Commission came to the conclusion that it would be premature to engage immediately in the preparation of a standard communication agreement and that it might be preferable to monitor developments in other organizations, particularly the Commission of the European Communities and the Economic Commission for Europe. It was pointed out that high-speed electronic commerce required a new examination of basic contract issues such as offer and acceptance, and that consideration should be given to legal implications of the role of central data managers in international commercial law.

134. After deliberation, the Commission decided that a session of the Working Group on International Payments would be devoted to identifying the legal issues involved and to considering possible statutory provisions, and that the Working Group would report to the Commission on the desirability and feasibility of undertaking

---

9. It may be noted that the Model Law is not intended to provide a comprehensive set of rules governing all aspects of electronic commerce. The main purpose of the Model Law is to adapt existing statutory requirements so that they would no longer constitute obstacles to the use of paperless means of communication and storage of information.

further work such as the preparation of a standard communication agreement.[10]

135. The Working Group on International Payments, at its twenty-fourth session, recommended that the Commission should undertake work towards establishing uniform legal rules on electronic commerce. It was agreed that the goals of such work should be to facilitate the increased use of electronic commerce and to meet the need for statutory provisions to be developed in the field of electronic commerce, particularly with respect to such issues as formation of contracts; risk and liability of commercial partners and third-party service providers involved in electronic commerce relationships; extended definitions of "writing" and "original" to be used in an electronic commerce environment; and issues of negotiability and documents of title (A/CN.9/360).

136. While it was generally felt that it was desirable to seek the high degree of legal certainty and harmonization provided by the detailed provisions of a uniform law, it was also felt that care should be taken to preserve a flexible approach to some issues where legislative action might be premature or inappropriate. As an example of such an issue, it was stated that it might be fruitless to attempt to provide legislative unification of the rules on evidence that may apply to electronic commerce massaging (ibid., para. 130). It was agreed that no decision should be taken at that early stage as to the final form or the final content of the legal rules to be prepared. In line with the flexible approach to be taken, it was noted that situations might arise where the preparation of model contractual clauses would be regarded as an appropriate way of addressing specific issues (ibid., para. 132).

137. The Commission, at its twenty-fifth session (1992), endorsed the recommendation contained in the report of the Working Group (ibid., paras. 129-133) and entrusted the preparation of legal rules on electronic commerce (which was then referred to as "electronic data interchange" or "EDI") to the Working Group on International Payments, which it renamed the Working Group on Electronic Data Interchange.[11]

138. The Working Group devoted its twenty-fifth to twenty-eighth sessions to the preparation of legal rules applicable to "electronic data interchange (EDI) and other modern means of

---

10. *Official Records of the General Assembly, Forty-sixth Session, Supplement No. 17* (A/46/17), paras. 311 to 317.

11. Ibid., *Forty-seventh Session, Supplement No. 17* (A/47/17), paras. 141 to 148.

communication" (reports of those sessions are found in documents A/CN.9/373, 387, 390 and 406).[12]

139. The Working Group carried out its task on the basis of background working papers prepared by the Secretariat on possible issues to be included in the Model Law. Those background papers included A/CN.9/WG.IV/WP.53 (Possible issues to be included in the programme of future work on the legal aspects of EDI) and A/CN.9/WG.IV/WP.55 (Outline of possible uniform rules on the legal aspects of electronic data interchange). The draft articles of the Model Law were submitted by the Secretariat in documents A/CN.9/WG.IV/WP.57, 60 and 62. The Working Group also had before it a proposal by the United Kingdom of Great Britain and Northern Ireland relating to the possible contents of the draft Model Law (A/CN.9/WG.IV/WP.58).

140. The Working Group noted that, while practical solutions to the legal difficulties raised by the use of electronic commerce were often sought within contracts (A/CN.9/WG.IV/WP.53, paras. 35–36), the contractual approach to electronic commerce was developed not only because of its intrinsic advantages such as its flexibility, but also for lack of specific provisions of statutory or case law. The contractual approach was found to be limited in that it could not overcome any of the legal obstacles to the use of electronic commerce that might result from mandatory provisions of applicable statutory or case law. In that respect, one difficulty inherent in the use of communication agreements resulted from uncertainty as to the weight that would be carried by some contractual stipulations in case of litigation. Another limitation to the contractual approach resulted from the fact that parties to a contract could not effectively regulate the rights and obligations of third parties. At least for those parties not participating in the contractual arrangement, statutory law based on a model law or an international convention seemed to be needed (see A/CN.9/350, para. 107).

---

12. The notion of "EDI and related means of communication" as used by the Working Group is not to be construed as a reference to narrowly defined EDI under article 2*(b)* of the Model Law but to a variety of trade-related uses of modern communication techniques that was later referred to broadly under the rubric of "electronic commerce". The Model Law is not intended only for application in the context of existing communication techniques but rather as a set of flexible rules that should accommodate foreseeable technical developments. It should also be emphasized that the purpose of the Model Law is not only to establish rules for the movement of information communicated by means of data messages but equally to deal with the storage of information in data messages that are not intended for communication.

141. The Working Group considered preparing uniform rules with the aim of eliminating the legal obstacles to, and uncertainties in, the use of modern communication techniques, where effective removal of such obstacles and uncertainties could only be achieved by statutory provisions. One purpose of the uniform rules was to enable potential electronic commerce users to establish a legally secure electronic commerce relationship by way of a communication agreement within a closed network. The second purpose of the uniform rules was to support the use of electronic commerce outside such a closed network, i.e., in an open environment. However, the aim of the uniform rules was to enable, and not to impose, the use of EDI and related means of communication. Moreover, the aim of the uniform rules was not to deal with electronic commerce relationships from a technical perspective but rather to create a legal environment that would be as secure as possible, so as to facilitate the use of electronic commerce between communicating parties.

142. As to the form of the uniform rules, the Working Group was agreed that it should proceed with its work on the assumption that the uniform rules should be prepared in the form of statutory provisions. While it was agreed that the form of the text should be that of a "model law", it was felt, at first, that, owing to the special nature of the legal text being prepared, a more flexible term than "model law" needed to be found. It was observed that the title should reflect that the text contained a variety of provisions relating to existing rules scattered throughout various parts of the national laws in an enacting State. It was thus a possibility that enacting States would not incorporate the text as a whole and that the provisions of such a "model law" might not appear together in any one particular place in the national law. The text could be described, in the parlance of one legal system, as a "miscellaneous statute amendment act". The Working Group agreed that this special nature of the text would be better reflected by the use of the term "model statutory provisions". The view was also expressed that the nature and purpose of the "model statutory provisions" could be explained in an introduction or guidelines accompanying the text.

143. At its twenty-eighth session, however, the Working Group reviewed its earlier decision to formulate a legal text in the form of "model statutory provisions" (A/CN.9/390, para. 16). It was widely felt that the use of the term "model statutory provisions" might raise uncertainties as to the legal nature of the instrument. While some support was expressed for the retention of the term "model statutory provisions", the widely prevailing view was that

the term "model law" should be preferred. It was widely felt that, as a result of the course taken by the Working Group as its work progressed towards the completion of the text, the model statutory provisions could be regarded as a balanced and discrete set of rules, which could also be implemented as a whole in a single instrument (A/CN.9/406, para. 75). Depending on the situation in each enacting State, however, the Model Law could be implemented in various ways, either as a single statute or in various pieces of legislation.

144. The text of the draft Model Law as approved by the Working Group at its twenty-eighth session was sent to all Governments and to interested international organizations for comment. The comments received were reproduced in document A/CN.9/409 and Add.1-4. The text of the draft articles of the Model Law as presented to the Commission by the Working Group was contained in the annex to document A/CN.9/406.

145. At its twenty-eighth session (1995), the Commission adopted the text of articles 1 and 3 to 11 of the draft Model Law and, for lack of sufficient time, did not complete its review of the draft Model Law, which was placed on the agenda of the twenty-ninth session of the Commission.[13]

146. The Commission, at its twenty-eighth session,[14] recalled that, at its twenty-seventh session (1994), general support had been expressed in favour of a recommendation made by the Working Group that preliminary work should be undertaken on the issue of negotiability and transferability of rights in goods in a computer-based environment as soon as the preparation of the Model Law had been completed.[15] It was noted that, on that basis, a preliminary debate with respect to future work to be undertaken in the field of electronic data interchange had been held in the context of the twenty-ninth session of the Working Group (for the report on that debate, see A/CN.9/407, paras. 106–118). At that session, the Working Group also considered proposals by the International Chamber of Commerce (A/CN.9/WG.IV/WP.65) and the United Kingdom of Great Britain and Northern Ireland (A/CN.9/WG.IV/WP.66) relating to the possible inclusion in the draft Model Law of additional provisions to the effect of ensuring that certain terms and conditions that might be incorporated in a data message by

---

13. *Official Records of the General Assembly, Fiftieth Session, Supplement No. 17* (A/50/17), para. 306.

14. Ibid., para. 307.

15. Ibid., *Forty-ninth Session, Supplement No. 17* (A/49/17), para. 201.

means of a mere reference would be recognized as having the same degree of legal effectiveness as if they had been fully stated in the text of the data message (for the report on the discussion, see A/CN.9/407, paras. 100–105). It was agreed that the issue of incorporation by reference might need to be considered in the context of future work on negotiability and transferability of rights in goods (A/CN.9/407, para. 103). The Commission endorsed the recommendation made by the Working Group that the Secretariat should be entrusted with the preparation of a background study on negotiability and transferability of EDI transport documents, with particular emphasis on EDI maritime transport documents, taking into account the views expressed and the suggestions made at the twenty-ninth session of the Working Group.[16]

147. On the basis of the study prepared by the Secretariat (A/CN.9/WG.IV/WP.69), the Working Group, at its thirtieth session, discussed the issues of transferability of rights in the context of transport documents and approved the text of draft statutory provisions dealing with the specific issues of contracts of carriage of goods involving the use of data messages (for the report on that session, see A/CN.9/421). The text of those draft provisions as presented to the Commission by the Working Group for final review and possible addition as part II of the Model Law was contained in the annex to document A/CN.9/421.

148. In preparing the Model Law, the Working Group noted that it would be useful to provide in a commentary additional information concerning the Model Law. In particular, at the twenty-eighth session of the Working Group, during which the text of the draft Model Law was finalized for submission to the Commission, there was general support for a suggestion that the draft Model Law should be accompanied by a guide to assist States in enacting and applying the draft Model Law. The guide, much of which could be drawn from the *travaux préparatoires* of the draft Model Law, would also be helpful to users of electronic means of communication as well as to scholars in that area. The Working Group noted that, during its deliberations at that session, it had proceeded on the assumption that the draft Model Law would be accompanied by a guide. For example, the Working Group had decided in respect of a number of issues not to settle them in the draft Model Law but to address them in the guide so as to provide guidance to States enacting the draft Model Law. The Secretariat

16. Ibid., *Fiftieth Session, Supplement No. 17* (A/50/17), para. 309.

was requested to prepare a draft and submit it to the Working Group for consideration at its twenty-ninth session (A/CN.9/406, para. 177).

149. At its twenty-ninth session, the Working Group discussed the draft Guide to Enactment of the Model Law (hereinafter referred to as "the draft Guide") as set forth in a note prepared by the Secretariat (A/CN.9/WG.IV/WP.64). The Secretariat was requested to prepare a revised version of the draft Guide reflecting the decisions made by the Working Group and taking into account the various views, suggestions and concerns that had been expressed at that session. At its twenty-eighth session, the Commission placed the draft Guide to Enactment of the Model Law on the agenda of its twenty-ninth session.[17]

150. At its twenty-ninth session (1996), the Commission, after consideration of the text of the draft Model Law as revised by the drafting group, adopted the following decision at its 605th meeting, on 12 June 1996:

"*The United Nations Commission on International Trade Law*,

"*Recalling* its mandate under General Assembly resolution 2205 (XXI) of 17 December 1966 to further the progressive harmonization and unification of the law of international trade, and in that respect to bear in mind the interests of all peoples, and in particular those of developing countries, in the extensive development of international trade,

"*Noting* that an increasing number of transactions in international trade are carried out by means of electronic data interchange and other means of communication commonly referred to as 'electronic commerce', which involve the use of alternatives to paper-based forms of communication and storage of information,

"*Recalling* the recommendation on the legal value of computer records adopted by the Commission at its eighteenth session, in 1985, and paragraph 5(b) of General Assembly resolution 40/71 of 11 December 1985 calling upon Governments and international organizations to take action, where appropriate, in conformity with the recommendation of the Commission[18] so as to ensure legal security in the context of the widest possible use of automated data processing in international trade,

"*Being of the opinion* that the establishment of a model law facilitating the use of electronic commerce, and acceptable to States with different legal, social and economic systems, contributes to the development of harmonious international economic relations,

---

17. Ibid., para. 306.

18. Ibid., *Fortieth Session, Supplement No. 17* (A/40/17), paras. 354–360.

"*Being convinced* that the UNCITRAL Model Law on Electronic Commerce will significantly assist all States in enhancing their legislation governing the use of alternatives to paper-based forms of communication and storage of information, and in formulating such legislation where none currently exists,

"1. *Adopts* the UNCITRAL Model Law on Electronic Commerce as it appears in annex I to the report on the current session;

"2. *Requests* the Secretary-General to transmit the text of the UNCITRAL Model Law on Electronic Commerce, together with the Guide to Enactment of the Model Law prepared by the Secretariat, to Governments and other interested bodies;

"3. *Recommends* that all States give favourable consideration to the UNCITRAL Model Law on Electronic Commerce when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based forms of communication and storage of information."[19]

---

19. Ibid., *Fifty-first Session, Supplement No. 17* (A/51/17), para. 209.

APPENDIX C

# (Australian) Electronic Transactions Bill 1999

*(Attorney-General)*

A Bill for an Act to facilitate electronic transactions, and for other purposes

# Electronic Transactions Bill 1999

*(Attorney-General)*

CONTENTS

**A Bill for an Act to facilitate electronic transactions, and for other purposes**

**The Parliament of Australia enacts:**

## Part 1
## Introduction

**1 Short title**

This Act may be cited as the Electronic Transactions Act 1999.

**2 Commencement**

(1) Subject to subsection (2), this Act commences on a day to be fixed by Proclamation.

(2) If this Act does not commence under subsection (1) within the period of 6 months beginning on the day on which this Act receives the Royal Assent, it commences on the first day after the end of that period.

**3 Object**

The object of this Act is to provide a regulatory framework that:

(a) recognises the importance of the information economy to the future economic and social prosperity of Australia; and

(b) facilitates the use of electronic transactions; and

(c) promotes business and community confidence in the use of electronic transactions; and

(d) enables business and the community to use electronic communications in their dealings with government.

**4 Simplified outline**

The following is a simplified outline of this Act:

- For the purposes of a law of the Commonwealth, a transaction is not invalid because it took place by means of one or more electronic communications.
- The following requirements imposed under a law of the Commonwealth can be met in electronic form:
  - (a) a requirement to give information in writing;
  - (b) a requirement to provide a signature;
  - (c) a requirement to produce a document;
  - (d) a requirement to record information;
  - (e) a requirement to retain a document.
- For the purposes of a law of the Commonwealth, provision is made for determining the time and place of the dispatch and receipt of an electronic communication.

- The purported originator of an electronic communication is bound by it for the purposes of a law of the Commonwealth only if the communication was sent by the purported originator or with the authority of the purported originator.

**5 Definitions**

(1) In this Act, unless the contrary intention appears:

**Commonwealth entity** means:

(a) a Minister; or
(b) an officer or employee of the Commonwealth; or
(c) a person who holds or performs the duties of an office under a law of the Commonwealth; or
(d) an authority of the Commonwealth; or
(e) an employee of an authority of the Commonwealth.

**consent** includes consent that can reasonably be inferred from the conduct of the person concerned.

**data** includes the whole or part of a computer program within the meaning of the *Copyright Act 1968*.

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

**electronic communication** means:

(a) a communication of information in the form of data, text or images by means of guided and/or unguided electromagnetic energy; or
(b) a communication of information in the form of speech by means of guided and/or unguided electromagnetic energy, where the speech is processed at its destination by an automated voice recognition system.

**information** means information in the form of data, text, images or speech.

**information system** means a system for generating, sending, receiving, storing or otherwise processing electronic communications.

**information technology requirements** includes software requirements.

**non-profit body** means a body that is not carried on for the purposes of profit or gain to its individual members and is, by the terms of the body's constitution, prohibited from making any distribution, whether in money, property or otherwise, to its members.

**place of business**, in relation to a government, an authority of a government or a non-profit body, means a place where any operations or activities are carried out by that government, authority or body.

**transaction** includes a transaction of a non-commercial nature.

(2) Before 1 July 2001, in this Act (other than this section):

**law of the Commonwealth** means a law of the Commonwealth specified in the regulations.

**6 Crown to be bound**

This Act binds the Crown in all its capacities.

**7 External Territories**

This Act extends to all the external Territories.

## Part 2
## Application of legal requirements to electronic communications

### Division 1—General rule about validity of transactions for the purposes of laws of the Commonwealth

**8 Validity of electronic transactions**

(1) For the purposes of a law of the Commonwealth, a transaction is not invalid because it took place wholly or partly by means of one or more electronic communications.

(2) The general rule in subsection (1) does not apply in relation to the validity of a transaction to the extent to which another, more specific provision of this Part deals with the validity of the transaction.

*Exemptions*

(3) The regulations may provide that subsection (1) does not apply to a specified transaction.

(4) The regulations may provide that subsection (1) does not apply to a specified law of the Commonwealth.

### Division 2—Requirements under laws of the Commonwealth

*Requirement to give information in writing*

**9 Writing**

(1) If, under a law of the Commonwealth, a person is required to give information in writing, that requirement is taken to have been met if the person gives the information by means of an electronic communication, where:

(a) in all cases—at the time the information was given, it was reasonable to expect that the information would be readily accessible so as to be useable for subsequent reference; and

(b) if the information is required to be given to a Commonwealth entity, or to a person acting on behalf of a Commonwealth entity, and the entity requires that the information be given,

in accordance with particular information technology requirements, by means of a particular kind of electronic communication—the entity's requirement has been met; and

(c) if the information is required to be given to a Commonwealth entity, or to a person acting on behalf of a Commonwealth entity, and the entity requires that particular action be taken by way of verifying the receipt of the information—the entity's requirement has been met; and

(d) if the information is required to be given to a person who is neither a Commonwealth entity nor a person acting on behalf of a Commonwealth entity—the person to whom the information is required to be given consents to the information being given by way of electronic communication.

*Permission to give information in writing*

(2) If, under a law of the Commonwealth, a person is permitted to give information in writing, the person may give the information by means of an electronic communication, where:

(a) in all cases—at the time the information was given, it was reasonable to expect that the information would be readily accessible so as to be useable for subsequent reference; and

(b) if the information is permitted to be given to a Commonwealth entity, or to a person acting on behalf of a Commonwealth entity, and the entity requires that the information be given, in accordance with particular information technology requirements, by means of a particular kind of electronic communication—the entity's requirement has been met; and

(c) if the information is permitted to be given to a Commonwealth entity, or to a person acting on behalf of a Commonwealth entity, and the entity requires that particular action be taken by way of verifying the receipt of the information—the entity's requirement has been met; and

(d) if the information is permitted to be given to a person who is neither a Commonwealth entity nor a person acting on behalf of a Commonwealth entity—the person to whom the information is permitted to be given consents to the information being given by way of electronic communication.

*Certain other laws not affected*

(3) This section does not affect the operation of any other law of the Commonwealth that makes provision for or in relation to requiring or permitting information to be given, in accordance with particular information technology requirements:

(a) on a particular kind of data storage device; or

(b) by means of a particular kind of electronic communication.

*Giving information*

(4) This section applies to a requirement or permission to give information, whether the expression **give**, **send** or **serve**, or any other expression, is used.

(5) For the purposes of this section, **giving information** includes, but is not limited to, the following:
- (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.

Note: Section 13 sets out exemptions from this section.

**10 Signature**

*Requirement for signature*

(1) If, under a law of the Commonwealth, the signature of a person is required, that requirement is taken to have been met in relation to an electronic communication if:
- (a) in all cases—a method is used to identify the person and to indicate the person's approval of the information communicated; and
- (b) in all cases—having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated; and
- (c) if the signature is required to be given to a Commonwealth entity, or to a person acting on behalf of a Commonwealth entity, and the entity requires that the method used as mentioned in paragraph (a) be in accordance with particular information technology requirements—the entity's requirement has been met; and
- (d) if the signature is required to be given to a person who is neither a Commonwealth entity nor a person acting on behalf of a Commonwealth entity—the person to whom the signature is required to be given consents to that requirement being met by way of the use of the method mentioned in paragraph (a).

*Certain other laws not affected*

(2) This section does not affect the operation of any other law of the Commonwealth that makes provision for or in relation to requiring:
- (a) an electronic communication to contain an electronic signature (however described); or

(b) an electronic communication to contain a unique identification in an electronic form; or
(c) a particular method to be used in relation to an electronic communication to identify the originator of the communication and to indicate the originator's approval of the information communicated.

Note: Section 13 sets out exemptions from this section.

**11 Production of document**

*Requirement to produce a document*

(1) If, under a law of the Commonwealth, a person is required to produce a document that is in the form of paper, an article or other material, that requirement is taken to have been met if the person produces, by means of an electronic communication, an electronic form of the document, where:
(a) in all cases—having regard to all the relevant circumstances at the time of the communication, the method of generating the electronic form of the document provided a reliable means of assuring the maintenance of the integrity of the information contained in the document; and
(b) in all cases—at the time the communication was sent, it was reasonable to expect that the information contained in the electronic form of the document would be readily accessible so as to be useable for subsequent reference; and
(c) if the document is required to be produced to a Commonwealth entity, or to a person acting on behalf of a Commonwealth entity, and the entity requires that an electronic form of the document be produced, in accordance with particular information technology requirements, by means of a particular kind of electronic communication—the entity's requirement has been met; and
(d) if the document is required to be produced to a Commonwealth entity, or to a person acting on behalf of a Commonwealth entity, and the entity requires that particular action be taken by way of verifying the receipt of the document—the entity's requirement has been met; and
(e) if the document is required to be produced to a person who is neither a Commonwealth entity nor a person acting on behalf of a Commonwealth entity—the person to whom the document is required to be produced consents to the production, by means of an electronic communication, of an electronic form of the document.

*Permission to produce a document*

(2) If, under a law of the Commonwealth, a person is permitted to produce a document that is in the form of paper, an article or other

material, then, instead of producing the document in that form, the person may produce, by means of an electronic communication, an electronic form of the document, where:

(a) in all cases—having regard to all the relevant circumstances at the time of the communication, the method of generating the electronic form of the document provided a reliable means of assuring the maintenance of the integrity of the information contained in the document; and

(b) in all cases—at the time the communication was sent, it was reasonable to expect that the information contained in the electronic form of the document would be readily accessible so as to be useable for subsequent reference; and

(c) if the document is permitted to be produced to a Commonwealth entity, or to a person acting on behalf of a Commonwealth entity, and the entity requires that an electronic form of the document be produced, in accordance with particular information technology requirements, by means of a particular kind of electronic communication—the entity's requirement has been met; and

(d) if the document is permitted to be produced to a Commonwealth entity, or to a person acting on behalf of a Commonwealth entity, and the entity requires that particular action be taken by way of verifying the receipt of the document—the entity's requirement has been met; and

(e) if the document is permitted to be produced to a person who is neither a Commonwealth entity nor a person acting on behalf of a Commonwealth entity—the person to whom the document is permitted to be produced consents to the production, by means of an electronic communication, of an electronic form of the document.

*Integrity of information*

(3) For the purposes of this section, the integrity of information contained in a document is maintained if, and only if, the information has remained complete and unaltered, apart from:

(a) the addition of any endorsement; or

(b) any immaterial change;

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

*Certain other laws not affected*

(4) This section does not affect the operation of any other law of the Commonwealth that makes provision for or in relation to requiring or permitting electronic forms of documents to be produced, in accordance with particular information technology requirements:

(a) on a particular kind of data storage device; or

(b) by means of a particular kind of electronic communication.

*Exemption*

(5) This section does not apply to a document required or permitted to be produced to a Commonwealth entity in connection with an application for the grant of a permission, certificate or similar thing, where the permission, certificate or thing is of a kind that is not capable of being granted to an Australian citizen.

*Copyright*

(6) The following provisions have effect:

(a) the generation of an electronic form of a document for the purposes of:

(i) this section; or

(ii) a law of a State or Territory that corresponds to this section;

does not constitute an infringement of the copyright in a work or other subject matter embodied in the document.

(b) the production, by means of an electronic communication, of an electronic form of a document for the purposes of:

(i) this section; or

(ii) a law of a State or Territory that corresponds to this section;

does not constitute an infringement of the copyright in a work or other subject matter embodied in the document.

Note: Section 13 sets out exemptions from this section.

**12 Retention**

*Recording of information*

(1) If, under a law of the Commonwealth, a person is required to record information in writing, that requirement is taken to have been met if the person records the information in electronic form, where:

(a) in all cases—at the time of the recording of the information, it was reasonable to expect that the information would be readily accessible so as to be useable for subsequent reference; and

(b) if the regulations require that the information be recorded, in electronic form, on a particular kind of data storage device—that requirement has been met.

*Retention of written document*

(2) If, under a law of the Commonwealth, a person is required to retain, for a particular period, a document that is in the form of paper, an article or other material, that requirement is taken to have been met if the person retains an electronic form of the document throughout that period, where:

(a) in all cases—having regard to all the relevant circumstances at the time of the generation of the electronic form of the document, the method of generating the electronic form of the

document provided a reliable means of assuring the maintenance of the integrity of the information contained in the document; and

(b) in all cases—at the time of the generation of the electronic form of the document, it was reasonable to expect that the information contained in the electronic form of the document would be readily accessible so as to be useable for subsequent reference; and

(c) if the regulations require that the electronic form of the document be retained on a particular kind of data storage device—that requirement has been met.

(3) For the purposes of subsection (2), the integrity of information contained in a document is maintained if, and only if, the information has remained complete and unaltered, apart from:

(a) the addition of any endorsement; or

(b) any immaterial change;

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

*Retention of electronic communications*

(4) If, under a law of the Commonwealth, a person (the **first person**) is required to retain, for a particular period, information that was the subject of an electronic communication, that requirement is taken to be met if the first person retains, or causes another person to retain, in electronic form, the information throughout that period, where:

(a) in all cases—at the time of commencement of the retention of the information, it was reasonable to expect that the information would be readily accessible so as to be useable for subsequent reference; and

(b) in all cases—having regard to all the relevant circumstances at the time of commencement of the retention of the information, the method of retaining the information in electronic form provided a reliable means of assuring the maintenance of the integrity of the information contained in the electronic communication; and

(c) in all cases—throughout that period, the first person also retains, or causes the other person to retain, in electronic form, such additional information obtained by the first person as is sufficient to enable the identification of the following:

(i) the origin of the electronic communication;

(ii) the destination of the electronic communication;

(iii) the time when the electronic communication was sent;

(iv) the time when the electronic communication was received; and

(d) in all cases—at the time of commencement of the retention of the additional information covered by paragraph (c), it was

reasonable to expect that the additional information would be readily accessible so as to be useable for subsequent reference; and

(e) if the regulations require that the information be retained, in electronic form, on a particular kind of data storage device—that requirement is met throughout that period.

(5) For the purposes of subsection (4), the integrity of information that was the subject of an electronic communication is maintained if, and only if, the information has remained complete and unaltered, apart from:

(a) the addition of any endorsement; or

(b) any immaterial change;

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

*Copyright*

(6) The generation of an electronic form of a document for the purposes of:

(a) this section; or

(b) a law of a State or Territory that corresponds to this section;

does not constitute an infringement of the copyright in a work or other subject matter embodied in the document.

Note: Section 13 sets out exemptions from this section.

**13 Exemptions from this Division**

*Exemptions under the regulations*

(1) The regulations may provide that this Division, or a specified provision of this Division, does not apply to a specified requirement.

(2) The regulations may provide that this Division, or a specified provision of this Division, does not apply to a specified permission.

(3) The regulations may provide that this Division, or a specified provision of this Division, does not apply to a specified law of the Commonwealth.

*Exemptions for courts and tribunals*

(4) This Division does not apply to the practice and procedure of a court or tribunal. For this purpose, **practice and procedure** includes all matters in relation to which rules of court may be made.

*Evidence Act 1995 etc not affected*

(5) This Division does not affect the operation of:

(a) the Evidence Act 1995; or

(b) a law of a State or Territory that corresponds to the *Evidence Act 1995*; or

(c) a law of a State or Territory, or a rule of common law, that makes provision for the way in which evidence is given in proceedings in a court.

**14 Time and place of dispatch and receipt of electronic communications**

*Time of dispatch*

(1) For the purposes of a law of the Commonwealth, if an electronic communication enters a single information system outside the control of the originator, then, unless otherwise agreed between the originator and the addressee of the electronic communication, the dispatch of the electronic communication occurs when it enters that information system.

(2) For the purposes of a law of the Commonwealth, if an electronic communication enters successively 2 or more information systems outside the control of the originator, then, unless otherwise agreed between the originator and the addressee of the electronic communication, the dispatch of the electronic communication occurs when it enters the first of those information systems.

*Time of receipt*

(3) For the purposes of a law of the Commonwealth, if the addressee of an electronic communication has designated an information system for the purpose of receiving electronic communications, then, unless otherwise agreed between the originator and the addressee of the electronic communication, the time of receipt of the electronic communication is the time when the electronic communication enters that information system.

(4) For the purposes of a law of the Commonwealth, if the addressee of an electronic communication has not designated an information system for the purpose of receiving electronic communications, then, unless otherwise agreed between the originator and the addressee of the electronic communication, the time of receipt of the electronic communication is the time when the electronic communication comes to the attention of the addressee.

*Place of dispatch and receipt*

(5) For the purposes of a law of the Commonwealth, unless otherwise agreed between the originator and the addressee of an electronic communication:
   (a) the electronic communication is taken to have been dispatched at the place where the originator has its place of business; and
   (b) the electronic communication is taken to have been received at the place where the addressee has its place of business.

(6) For the purposes of the application of subsection (5) to an electronic communication:
   (a) if the originator or addressee has more than one place of business, and one of those places has a closer relationship to

the underlying transaction—it is to be assumed that that place of business is the originator's or addressee's only place of business; and

(b) if the originator or addressee has more than one place of business, but paragraph (a) does not apply—it is to be assumed that the originator's or addressee's principal place of business is the originator's or addressee's only place of business; and

(c) if the originator or addressee does not have a place of business—it is to be assumed that the originator's or addressee's place of business is the place where the originator or addressee ordinarily resides.

*Exemptions*

(7) The regulations may provide that this section does not apply to a specified electronic communication.

(8) The regulations may provide that this section does not apply to a specified law of the Commonwealth.

**15 Attribution of electronic communications**

(1) For the purposes of a law of the Commonwealth, unless otherwise agreed between the purported originator and the addressee of an electronic communication, the purported originator of the electronic communication is bound by that communication only if the communication was sent by the purported originator or with the authority of the purported originator.

(2) Subsection (1) is not intended to affect the operation of a law (whether written or unwritten) that makes provision for:

(a) conduct engaged in by a person within the scope of the person's actual or apparent authority to be attributed to another person; or

(b) a person to be bound by conduct engaged in by another person within the scope of the other person's actual or apparent authority.

*Exemptions*

(3) The regulations may provide that this section does not apply to a specified electronic communication.

(4) The regulations may provide that this section does not apply to a specified law of the Commonwealth.

*Certain provisions of the Evidence Act 1995 etc not affected*

(5) This section does not affect the operation of:

(a) section 87 or 88 of the *Evidence Act 1995*; or

(b) a law of a State or Territory that corresponds to section 87 or 88 of the *Evidence Act 1995*; or

(c) a law of a State or Territory, or a rule of common law, that provides for a statement made by a person to be treated as an admission made by a party to a proceeding in a court.

## Part 3
## Miscellaneous

**16 Regulations**

The Governor-General may make regulations prescribing matters:

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

(b) necessary or convenient to be prescribed for carrying out or giving effect to this Act.

---

APPENDIX D

# Extracts from the Evidence Code relating to documentary evidence and evidence produced by machines, devices or technical processes

## PART 6
## DOCUMENTARY EVIDENCE AND EVIDENCE PRODUCED BY MACHINE, DEVICE OR TECHNICAL PROCESS

**117 Offering documents in evidence without calling a witness**

(1) A party may give notice in writing to every other party that the party proposes to offer a document, including a public document, as evidence in the proceeding without calling a witness to produce the document. A copy of the document must be attached to the notice.

(2) A party who on receiving a notice wishes to object to the authenticity of the document to which the notice refers or to the fact that it is to be offered in evidence without being produced by a witness must give a notice of objection in writing to every other party.

(3) If no party objects to a proposal to offer a document as evidence without calling a witness to produce it or if the judge dismisses an objection to the proposal, the document, if otherwise admissible, may be admitted in evidence and it will be presumed, in the absence of evidence to the contrary, that the nature, origin, and contents of the document are as shown on its face.

(4) A party must give notice of a proposal to offer a document without calling a witness to produce it

(a) a sufficient time before the hearing to provide all the other parties with a fair opportunity to consider the proposal; or

(b) within such time, whether before or after the commencement of the hearing, as the judge may allow and subject to any conditions that the judge may impose.

(5) A party must give notice of objection to a proposal to offer a document without calling a witness to produce it

(a) a sufficient time before the hearing to provide all the other parties with a fair opportunity to consider the notice; or

(b) within such time, whether before or after the commencement of the hearing, as the judge may allow and subject to any conditions that the judge may impose.

*Section 117 continues overleaf*

# PART 6
# DOCUMENTARY EVIDENCE AND EVIDENCE PRODUCED BY MACHINE, DEVICE OR TECHNICAL PROCESS

C406 This Part of the Code contains provisions on the admissibility and authenticity of documentary evidence. It also contains a provision about evidence produced by a machine, device or technical process.

C407 Part 6 aims to simplify, shorten and clarify the existing rules. Current technology can assure accuracy in many instances without the need to produce the original, and indeed, it is often impossible to distinguish a copy from the original. It will, of course, always remain open to a party to dispute the accuracy of secondary evidence.

C408 If the authenticity of documents is not in dispute, as is often the case – especially in civil proceedings – the Code allows the documents to be admitted without the need to produce them through a witness – *s 117*. This follows logically from *s 13*, which allows a judge to look at a document and draw inferences about authenticity from the document itself.

C409 The provisions contained in this Part have no bearing on the application of the hearsay rule. The two rules are complementary. Unless the operation of the hearsay rules is expressly excluded, any document that contains hearsay must also comply with the hearsay rule in the Code.

## Section 117 Offering documents in evidence without calling a witness

C410 *Section 117* is intended to simplify the process of producing documents in evidence, including public documents (defined in *s 4*). This section introduces a new procedure whereby a party who wishes to offer a document in evidence without calling a witness to produce the document, gives notice of its intention to do so and annexes a copy of the document to the notice. It is expected that in the case of a paper document (as opposed to an audiotape or video record) the copy will be a photocopy. If no other party objects, or if the judge dismisses the objection, the document will be admitted and will be presumed to be what it purports to be and to contain what it purports to contain on its face.

*Section 117 commentary continues overleaf*

6) The judge may dispense with the requirement to give notice under subsection (1) or (2) on such conditions as the judge may impose.

Definitions: **copy**, **document**, **judge**, **party**, **proceeding**, **public document**, **witness**, s 4.

**118 Summary of voluminous documents**

(1) A party may, with the permission of the judge, give evidence of the contents of a voluminous document or a voluminous compilation of documents by means of a summary or chart.

(2) A party offering evidence by means of a summary or chart must, if the judge so directs on the request of another party or on the judge's own initiative, either produce the voluminous document or compilation of documents for examination in court during the hearing or make it available for examination and copying by other parties at a reasonable time and place.

Definitions: **document**, **judge**, **offer evidence**, **party**, s 4.

C411 The notice requirement is in addition to any disclosure that occurred during discovery. Its purpose is to indicate to other parties which documents will be produced in evidence without calling a witness to produce them. Compliance should be a simple matter. For instance, parties may indicate by reference to the list of documents provided at discovery which documents will be produced in this way.

C412 Both notice and counter-notice must be given in sufficient time before a hearing to enable other parties to consider the issues, or within the time the judge allows. This is to promote efficiency and economy by ensuring that problems are dealt with before the hearing. However, the judge has a discretion to allow notice to be given even after the hearing has commenced.

C413 Under *s 117(6)*, the judge may dispense with notice altogether, subject to any conditions thought necessary. *Subsection (6)* also enables the judge to develop a specific regime for a particular case – for example, a complex case with a large volume of documents. This may be done in the context of a system of case management or an application for directions under Rules 438 or 446H of the High Court Rules or Rule 434 of the District Courts Rules.

C414 The procedural requirements in *s 117* are additional to the admissibility requirements elsewhere in the Code; for example, the hearsay rules.

### Section 118 Summary of voluminous documents

C415 *Section 118* allows a party, with the permission of the judge, to produce the contents of a voluminous document or compilation of documents in the form of a summary or chart. The section is modelled on Rule 1006 of the United States Federal Rules of Evidence and is designed to meet a practical need. *Section 118(2)* obliges a party who has given evidence in this way to produce (if the judge so directs) the voluminous document in court or elsewhere at a reasonable time and place for examination by other parties.

**119 Translations and transcripts**

(1) A party may offer a document which purports to be a translation into English of a document in a language other than English if notice is given to all other parties a sufficient time before the hearing to provide those other parties with a fair opportunity to scrutinise the translation.

(2) The translation will be presumed to be an accurate translation unless evidence sufficient to raise doubt about the presumption is offered.

(3) A party may offer a document which purports to be a transcript of information or other matter that is recorded

(a) in a code (including shorthand writing or programming code); or

(b) in such a way as to be capable of being reproduced as sound or script,

if notice is given to all other parties a sufficient time before the hearing to provide those other parties with a fair opportunity to scrutinise the transcript.

(4) A party who offers a transcript of information or other matter in a sound recording under subsection (3) must play all or part of the sound recording in court during the hearing if the sound recording is available and the judge so directs, either on the application of another party or on the judge's own initiative.

---

Definitions: **document**, **judge**, **party**, s 4.

**120 Proof of signatures on attested documents**

The signature, execution or attestation of a document (including a testamentary document) that is required by law to be attested may be proved by any satisfactory means and an attesting witness need not be called to prove that the document was signed, executed or attested (whether by handwriting, digital means or otherwise) as it purports to have been signed, executed or attested.

---

Definitions: **document**, **witness**, s 4.

## Section 119 Translations and transcripts

C416 *Section 119(1)* and *(2)* introduce a presumption that a translation into English of a document in another language is an accurate translation if notice is given in sufficient time before the hearing to enable other parties to examine the translation. For the presumption to apply, however, the contents of the original document must be admissible under the Code.

C417 *Section 119(3)* enables a party to offer evidence of information recorded in a code, sound recording or script (such as a microfiche) in the form of a transcript. The words "information or other matter" are deliberately wide in order to include matter not consisting of words – for example, figures, symbols, music and other sounds, such as radar blips. However, the transcript will be admissible only if the information it transcribes is admissible. The notice requirement will enable opposing parties to apply to have the sound recording played in whole or in part if the accuracy of the transcript is in doubt.

## Section 120 Proof of signatures on attested documents

C418 *Section 120* is based on s 18 of the Evidence Act 1908. It abrogates the old rule that one of the subscribing witnesses to an attested document must be called unless all such witnesses are unavailable. *Section 120* allows any relevant evidence of due execution or attestation to be given to prove these issues, whether or not the attesting witness is available. Unlike s 18 of the Evidence Act 1908, *s 120* applies to wills.

**121 Evidence produced by machine, device or technical process**

(1) If a party offers evidence that was produced wholly or partly by a machine, device, or technical process and the machine, device, or technical process is of a kind that ordinarily does what a party asserts it to have done, it is presumed that on a particular occasion the machine, device, or technical process did what that party asserts it to have done, unless another party offers evidence sufficient to raise a doubt about the presumption.

(2) If information or other matter is stored in such a way that it cannot be used by the court unless a machine, device, or technical process is used to display, retrieve, produce or collate it, a party may offer a document that was or purports to have been displayed, retrieved, or collated by use of the machine, device, or technical process.

---

Definitions: **document**, **offer evidence**, **party**, s 4.

## Section 121 Evidence produced by machine, device or technical process

C419 The general words "machine, device or technical process" are intended to encompass technological developments, both current and future. A "machine" or a "device" will include, for example, a photocopier, a computer, word processor or a fax machine. "Technical process" is intended to cover a chemical or other process that might not aptly be described as carried out by a machine or device.

C420 In outline, *s 121* provides that if the proponent of machine-produced evidence adduces evidence of the operation that a machine of that kind ordinarily performs (or if the fact-finder is able to take judicial notice of the machine's operation), it is presumed that on the particular occasion the machine did what it ordinarily does. The presumption is rebuttable by evidence sufficient to raise a doubt about it, a lower standard than the formula "evidence to the contrary".

C421 The objective of the presumption is to facilitate the proof of documents and other things by reducing the need for complex and expensive technical evidence about the workings of a machine when those matters are not seriously in issue. When the presumption is successfully challenged, in addition to evidence on the workings of the class of machines to which the particular machine belongs, the proponent will also have to offer evidence that the particular machine was reliable and was properly operated on the occasion in question. This will enable the fact-finder to infer what would otherwise be presumed: ie, that on the occasion in question, the machine did what it ordinarily does.

C422 *Section 121(2)* offers a practical solution to the obvious problem that information stored in a computer or on microfiche, for example, or on sound and video recordings, cannot be accessed without display on a screen or conversion to paper form. The subsection provides that a party may offer a document that purports to display, retrieve or collate such information. "Document" is widely defined in *s 4*.

C423 The hearsay and other rules apply to evidence produced by machines. The effect of *s 5* is that *s 121* will be overridden by other legislative provisions on evidence produced by machines.

**122 Authenticity of public documents**

(1) A document that purports to be a public document, or a copy of or an extract from or a summary of a public document, and to have been

(a) sealed with the seal of a person or a body that might reasonably be supposed to have the custody of that public document; or

(b) certified to be such a copy, extract or summary by a person who might reasonably be supposed to have the custody of that public document,

is presumed, unless the contrary is proved, to be a public document or a copy of the public document or an extract from or summary of the public document, and may be offered in evidence to prove the truth of its contents.

(2) Subpart 1 of Part 3 (hearsay evidence) does not apply to evidence offered under this section.

---

Definitions: **copy**, **document**, **public document**, **seal**, s 4.

## Section 122 Authenticity of public documents

C424 *Section 122(1)* contains a rebuttable presumption that a sealed public document ("public document" is defined in *s 4*) or a certified copy ("copy" is also defined in *s 4*), extract or summary of a public document is presumed to be what it purports to be. The seal must be the seal of a person or body that might reasonably be supposed to have the custody of the public document – for example the Clerk of the House of Representatives may reasonably be supposed to have the custody of Acts of Parliament. Similarly, the certification must be by such a person.

C425 The effect of *s 122(2)* is that a sealed public document or a certified copy of a public document is admissible to prove the truth of its contents without the restrictions of the hearsay rule.

**123 Evidence of convictions, acquittals, and other judicial proceedings**

(1) Evidence of the following facts, where admissible, may be given by a certificate purporting to be signed by a judge, a registrar or other officer having custody of the court records:

(a) the conviction or acquittal of a person charged with an offence and the particulars of the offence and of the person, including the name and date of birth of a natural person and the name and date and place of incorporation of a body corporate;

(b) the sentencing by a court of a person to any penalty and the particulars of the offence for which that person was sentenced and of the person, including the name and date of birth of a natural person and the name and date and place of incorporation of a body corporate;

(c) an order or judgment of a court and the nature, parties and particulars of the proceeding to which the order or judgment relates;

(d) the existence of a criminal or civil proceeding, whether or not the proceeding has been concluded and the nature of the proceeding.

(2) A certificate under this section is sufficient evidence of the facts stated in it without proof of the signature or office of the person appearing to have signed the certificate.

(3) The manner of proving the facts referred to in subsection (1) authorised by this section is in addition to any other manner of proving any of those facts authorised by law.

(4) If a certificate under this section is offered in evidence in a proceeding for the purpose of proving the conviction or acquittal of a person, or the sentence by a court of a person to a penalty, or an order made by a court concerning a person, and the name of the person stated in the certificate is substantially similar to the name of the person concerning whom the evidence is offered, it is presumed, in the absence of evidence to the contrary, that the person whose name is stated in the certificate is the person concerning whom the evidence is offered.

(5) Subpart 1 of Part 3 (hearsay evidence) does not apply to evidence offered under this section.

---

Definitions: **conviction**, **judge**, **party**, **proceeding**, s 4.

## Section 123 Evidence of convictions, acquittals, and other judicial proceedings

C426 This provision sets out the means by which convictions, acquittals, sentences, judgments, orders or pending proceedings may be proved, once it has been determined that evidence of the conviction, acquittal, sentence, judgment, order or pending proceeding is admissible.

C427 When a fact described in any of the paragraphs in *s 123(1)* is admissible, that fact may be proved by means of a certificate signed by the person with custody of court records. The certificate will in itself be sufficient to prove the existence of that fact. It will not be necessary to prove the signature or office of the signatory.

C428 *Section 123(4)* provides a convenient way of proving the identity of the person about whom the facts referred to in *subs (1)* are sought to be proved. If the name in a certificate given under *subs (1)* is substantially similar to the name of the person about whom such a fact is sought to be proved, it is presumed that that person was the person named in the certificate. The presumption can be rebutted by evidence to the contrary.

C429 Since the hearsay rule does not apply, a certificate issued under *subs (1)* is admissible to prove the truth of its contents, unless the evidence is precluded by any other provision in the Code.

APPENDIX E

# Overseas developments relating to electronic signatures since ECom 1

## Singapore

*Electronic Transactions Act 1998*

E1 THE ACT PROVIDES that where a rule of law requires a signature, or provides consequences if a document is not signed then an "electronic signature" satisfies that rule of law (section 8). "Electronic signature" is defined in section 2. Section 4 provides that the Act does not apply to any rule of law requiring writing or signatures in relation to wills, negotiable instruments, declarations of trust, documents of title, powers of attorney, indentures and instruments for dealings in land. These exceptions may be amended by regulation made under section 4(2). Section 5 provides that Parts 2 and 4 may be varied by consent of the parties. It enacts article 4 of the Model Law.

E2 The Act also establishes a regime of "secure electronic signatures". Section 18 provides that in any proceeding involving a "secure electronic signature", it shall be presumed that the secure electronic signature is the signature of the person to whom it correlates and that the secure electronic signature was affixed by that person with the intention of signing or approving the electronic record. The Act sets out when a signature will be considered a "secure electronic signature" (sections 17, 20).

E3 The Act sets out the representations which a certification authority makes by issuing a certificate (section 30); sets out rules in relation to the revocation and suspension of certificates by a certification authority (sections 31–35); places obligations on subscribers for certificates (section 37); places an obligation on subscribers to exercise reasonable care to retain control of the private key corresponding to the public key listed in the certificate and prevent its disclosure to others (section 39) and to notify the certification

authority if the private key is compromised (section 40); sets out presumptions which apply in relation to certificates (section 21); provides rules in relation to the allocation of risk for invalid digital signatures (section 22); sets out when reliance on a digital signature is foreseeable (section 23); and creates a number of criminal offences (sections 25, 26). The Act also regulates certification authorities (see, for instance sections 41 and 42) and provides rules in relation to the liability of certification authorities.

## Australia

### *Electronic Transactions Bill 1999*

E4 Section 10 of the Electronic Transaction Bill is in substantially the same terms as article 7(1) of the Model Law. Section 13 provides that regulations may provide that section 10 shall not apply to a particular law. The Bill also sets out rules for the time and place of dispatch of electronic communications (section 14) and in relation to attribution of electronic messages (section 15). The Electronic Transactions Bill is reproduced as appendix C.

## Canada

### *Uniform Electronic Commerce Act*

E5 Section 10 of the Uniform Act is similar to article 7(1) of the UNCITRAL Model Law. Section 10 provides:

> A requirement under [enacting jurisdiction] law for the signature of a person is satisfied by an electronic signature if–
> (a) the electronic signature is reliable for the purpose of identifying the person, in the light of all the circumstances, including any relevant agreement and the time the electronic signature was made;
> (b) the association of the electronic signature to the relevant electronic document is reliable for the purpose for which the electronic document was made, in the light of all the circumstances, including any relevant agreement and the time the electronic signature was made; and
> (c) where the signature or signed document is to be provided to the Government,
> (i) the Government or the part of Government to which the information is to be provided has consented to accept electronic signatures; and
> (ii) the electronic document meets the information technology standards and requirements as to method and as to reliability of the signature, if any, established by the Government or part of Government as the case may be.

E6 The section 1(b) definition of "electronic signature" is expressed in technologically-neutral language. Section 2(3) of the Act provides that nothing in the Act applies to wills and their codicils, trusts created by wills, powers of attorney, negotiable instruments, or dealings and interests in land. The Act has been drafted by the Uniform Law Conference of Canada, which promotes the harmonisation of Canadian legislation. The Act will not however become law until it is adopted by one or more of Canada's provinces or territories.

### *Personal Information Protection and Electronic Documents Bill*

E7 This Bill was due to receive its second reading in the Canadian Parliament on 4 November 1999. The provisions relating to electronic documents will apply to federal statutes and regulations only. "Electronic signature" is defined in section 31(1) as meaning

> a signature that consists of one or more letters, characters, numbers or other symbols in digital form incorporated in, attached to or associated with an electronic document.

The Bill goes on to provide in section 43 that a requirement under a federal law for a signature will be satisfied by an electronic signature, provided the relevant regulations have been complied with.

## United States

### *Draft Uniform Electronic Transactions Act*

E8 In March 1999 the National Conference of Commissioners on Uniform State Laws published a Draft Uniform Electronic Transactions Act. The draft provides that a record or signature may not be denied legal effect or enforceability solely because it is in electronic form (section 106). Section 106(d) provides that if a law requires a signature the law is satisfied with respect to an electronic record if the electronic record includes an electronic signature. The draft does not relate to electronic signatures for wills, codicils, or testamentary trusts (section 103). Section 110 provides that if a law requires that a signature be notarised or acknowledged, the law is satisfied with respect to an electronic signature if a security procedure was applied which establishes the identity of the person signing the electronic record and that the electronic record had not been altered since it was electronically signed.

### *Illinois Electronic Commerce Security Act 1998*

E9 Section 5–120 provides that an electronic signature will, generally, satisfy a rule of law where the law requires a signature. However, a number of exceptions are created. For instance, the provisions of the section do not apply to any rule of law governing the creation or execution of a will, trust, living will, healthcare power of attorney, negotiable instrument or instrument of title.

E10 The Act also sets up a regime of "secure electronic signatures". The Act provides that in civil disputes, it shall be rebuttably presumed that a secure electronic signature is the signature of the person to whom it correlates (section 10–120). The Act sets out detailed requirements for an electronic signature to be classified as a "secure electronic signature" (sections 10–110, 10–135, 15–105).

E11 The Act places duties on those generating and using "signature devices" (section 10–125); creates offences in relation to the unauthorised use of "signature devices" (sections 10–140, 15–220); sets out when reliance on "certificates" will be foreseeable (section 15–205); prohibits publication of certificates in certain circumstances (section 15–205); creates offences in relation to the use of certificates (sections 15–210, 15–215); requires certain disclosures to be made by certification authorities (section 15–305); sets out the representations which are made by certification authorities by issuing a certificate (section 15–315); sets out when a certificate must be revoked (section 15–320); provides rules in relation to the admissibility of electronic signatures (section 5–130); sets out rules in relation to the attribution of secure electronic signatures (section 10–130) and places duties on the subscribers of certificates (section 20–101).

### *Minnesota Electronic Authentication Act 1998*

E12 Section 325K.19(a) provides that where a rule of law requires a signature, or provides for certain consequences in the absence of a signature, that rule is satisfied by a digital signature if certain requirements are met. "Digital signature" is defined in section 325K.01.

E13 The Minnesota statute provides for and regulates certification authorities. For instance, the Act sets out rules in relation to audits of certification authorities (section 325K.06), the investigation of certification authorities (section 325K.07), the suspension and revocation of licences for certification authorities (section 325.K.07), the issuance, revocation and suspension of

certificates (section 325K.10, section 325K.16), and also rules as to the warranties and obligations imposed on a certification authority by the issuance of a certificate (section 325K.11). The Act also sets out what an organisation must do to be able to obtain a licence to be a certification authority (section 325K.05), provides that parties may provide for the effectiveness and enforceability of digital signatures by contract (section 325K.05), sets out the representations which are made by a subscriber for a certificate (section 325K.12), and provides rules in relation to the allocation of risk (section 325K.20).

### *Missouri Digital Signatures Act 1998*

E14 The Missouri Digital Signature Act 1998 is in substantially the same terms as the Minnesota Electronic Authentication Act 1998.

## European Commission

E15 In May 1988 a document entitled "A Proposal for a European Parliament and Council Directive on a Common Framework for Electronic Signatures" was released. The Directive covers the legal recognition of electronic signatures.

E16 Article 5 of the Directive provides that Member States must ensure that an "electronic signature" is not denied legal effect, validity or enforceability solely on the grounds that the signature is in electronic form, is not based upon a "qualified certificate", or is not based upon a certificate issued by an accredited "certification service provider". Article 5 also provides that Member States must ensure that electronic signatures which are based on a qualified certificate issued by a certification service provider are recognised as satisfying the legal requirement of a hand written signature and are admissible as evidence in legal proceedings in the same manner as hand written signatures.

E17 Article 3 provides that Member States must not make the provision of certification services subject to prior authorisation. However, Member States may introduce or maintain voluntary accreditation schemes aimed at enhancing levels of certification service provision. Article 6 sets out the liability of certification service providers which issue qualified certificates. Article 7 provides that Member States must ensure that certificates issued by a certification service provider established in a third country are recognised as legally equivalent to certificates issued by a certification service provider established within the European Community as long as certain requirements are met.

## Korea

### *Electronic Transaction Law*

E18 Article 5 provides that an electronic message shall not be denied legal validity on the ground that it is in electronic form. "Electronic Message" is defined in article 2. Article 6 provides that a digital signature certified by an authorised certification authority is deemed a valid signature or seal as prescribed by relevant laws. "Digital signature" is also defined in article 2. Article 16 provides that the government may designate an authorised certification authority to ensure the security and reliability of electronic commerce.

---

# Select bibliography

## REPORTS


APEC Telecommunications Working Group *Authentication 99/SGEC/017* (seminar delivered at Asia Pacific Economic Cooperation Conference, Auckland, 27–28 June 1999)

Asia Pacific Economic Cooperation *Blueprint for Action of Electronic Commerce* (Kuala Lumpur, 1988)

Attorney-General's Department *An Australian Legal Framework for Electronic Commerce (Issues Paper)* (Canberra, 1998) at <http://www.law.gov.au/ecommerce/issues_11_98.html>

Australian Law Reform Commission *Annual Report 1998 R86* (Australia Government Publishing Service, Canberra, 1998)

Australian Securities and Investments Commission Working Group *Discussion Paper on an Expanded EFT Code of Practice* (26 July 1998) at <http://www.asic.gov.au/publications>

S Baker and M Yeo *Trends in International Authentication Legislation: A Report Prepared for the Internet Law and Policy Forum* (Steptoe & Johnson, Washington, 1999)

Banking Ombudsman's *Annual Report 1997/1998*

Hon Justice Baragwanath "A Call for Joint Action to Make Changes in International and Domestic Law which are Critical to a Borderless World of Electronic Commerce" (address to APEC Conference, Kuala Lumpur, Singapore, 21 October 1998) at <http://www.lawcom.govt.nz/speeches/apececom211098.htm>

Hon Justice Baragwanath "Changes in International and Domestic Law Which are Critical to a Borderless World of Electronic Commerce: An Update" (paper presented to APEC/WTC meeting, APEC Conference, Auckland, 6 September 1999) <http://www.lawcom.govt.nz/speech_index.html>

Hon Justice Baragwanath, "Global Electronic Commerce: the Response of the Law Commission" (paper presented to New Zealand Law Conference 1999, Rotorua, New Zealand, 6–10 April 1999)

M Bayly *Towards Electronic Data Interchange in Trade: (1) The Impact of System Architecture on Documentary Certainty and (2) Contiguity with Existing Business Practice (a Focus on the Bill of Lading)* (University of Auckland, Auckland, 1997)

Commission on Enterprise, Business Facilitation and Development "Legal Dimensions of Electronic Commerce" in *Expert Meeting on Capacity Building in the Area of Electronic Commerce: Legal and Regulatory Dimensions TD/B/EOM.3/EM.8/2* (Report of the UNCTAD Secretariat, Geneva, 1999)

Corporate Law Economic Reform *Electronic Commerce: Cutting Cyberspace – Building Businesses* (Printing Division of the Can Print Communications Pty Limited, Canberra, 1997)

Crimes Consultative Committee *Crimes Bill 1999, Report of the Crimes Consultative Committee* (Wellington, April 1991)

G Crowhen and S Grace "The Legal Implications of Doing Business Electronically: Business Application of the Law of Contract to E-Commerce" (paper presented to Institute for International Research Conference, Auckland and Wellington, 24–25 February, 1999)

Department of Foreign Affairs and Trade *Putting Australia on the New Silk Road* (Canberra, 1997)

Department of Trade and Industry *Building Confidence in Electronic Commerce: A Consultation* (London, 1999) at <http://www.dti.gov.uk/cii/elec/elec_com.html>

Electronic Commerce Expert Group *Electronic Commerce: Building the Legal Framework* (Australia, 1998) at http://www.law.gov.au/aghome/advisory/eceg

D Goddard "Global Disputes – Jurisdiction, Interim Relief and Enforcement of Judgments" (paper presented to New Zealand Law Society Conference, Rotorua, April 1999)

Information Industries Taskforce *The Global Information Economy: the Way Ahead* (Department of Industry, Australia, 1997)

Information Technology Association of New Zealand *Annual Report* (Wellington, 1998)

Inland Revenue Department *GST – A Review (discussion paper)* (Wellington, 1999)

L Longdin "Digital Transmissions and the Liability of On-Line Service Providers" (paper presented to the Fay, Richwhite Conference, Auckland, 15–16 July, 1999)

Ministerial Council for the Information Economy *Towards an Australian Strategy for the Information Economy* (Office for the Information Economy, Canberra, 1998)

Ministry of Commerce *Bright Future: 5 Steps Ahead: Making ideas work for New Zealand* (Wellington, 1999)

Ministry of Commerce *Electronic Commerce: The Freezer Ship of the 21st Century* (Wellington, 1998)

Ministry of Consumer Affairs *Electronic Commerce and the New Zealand Consumer: Issues and Strategies for the Future (discussion paper)* (Wellington, 1997)

New Zealand Law Commission *A New Interpretation Act: To Avoid "Prolixity and Tautology": NZLC R17* (Wellington, 1990)

New Zealand Law Commission *Crown Liability and Judicial Immunity: A Response to Baigent's case and Harvey v Derrick: NZLC R37* (Wellington, 1997)

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

New Zealand Law Commission *Dishonestly Procuring Valuable Benefits: NZLC R51* (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 *Justice: The Experiences of Maori Women Te Tikanga o te Ture: Te Mātauranga o ngā Wāhine Māori e pa ana ki tēnei: NZLC R53* (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 *Evidence Law: Documentary Evidence and Judical Notice: NZLC PP22* (Wellington, 1994)

New Zealand Law Commission *Repeal of the Contracts Enforcement Act 1956: NZLC PP30* (Wellington, 1997)

New Zealand Law Commission *Women's Access to Legal Services: NZLC SP1* (Wellington, 1999)

Office of the Minister for Information Technology "Electronic Commerce", Report to Government Strategy Committee (Wellington, 1998)

Office of the Ombudsman *Annual Report 1997–1998* (Wellington, 1998)

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

Office of the Privacy Commissioner "Privacy Protection: The Key to Electronic Commerce" (seminar delivered at Asia Pacific Economic Cooperation Conference, Auckland, 27–28 June 1999)

Office of the Privacy Commissioner *Review of the Privacy Act: A background paper* (Wellington, 1998)

Public Record Office *Final Report of the Victorian Electronic Records Strategy* (Victoria, 1998)

M Sneddon "Risk Allocation in Electronic Banking: Lessons for Electronic Commerce" (paper presented to the New Zealand Law Conference 1999, Rotorua 6–10, April 1999)

Steering Group on Electronic Commerce *Electronic Commerce in APEC Fora (APEC Secretariat) 99/SGEC/015* (seminar delivered at Asia Pacific Economic Cooperation Conference, Auckland, 27–28 June 1999)

Steering Group on Electronic Commerce *Electronic Commerce Law Guide: Overview of E-Com Law 99/SGEC/016* (seminar delivered at Asia Pacific Economic Cooperation Conference, Auckland, 27–28 June 1999)

Steering Group on Electronic Commerce *Global Commerce Needs Global Commercial Law (UNCITRAL) 99/SGEC/011* (seminar delivered at Asia Pacific Economic Cooperation Conference, Auckland, 27–28 June 1999)

Steering Group on Electronic Commerce *Measuring E-Commerce 99/SGEC/018* (seminar delivered at Asia Pacific Economic Cooperation, Auckland, 27–28 June 1999)

Steering Group on Electronic Commerce *The Work of the OECD on Electronic Commerce 99/SGEC/005* (seminar delivered at Asia Pacific Economic Cooperation Conference, Auckland, 27–28 June 1999)

P Sumpter and A Poole *An Overview of Legal Issues 99/SGEC/027* (seminar delivered at Asia Pacific Economic Cooperation Conference, Auckland, 27–28 June 1999)

UNCITRAL Working Group on Electronic Commerce 35th session, (September 1999) at <www.uncitral.org>

United Nations Commission on International Trade Law *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment* (United Nations, New York, 1997)

United Nations Commission on International Trade Law *Uniform Commercial Law in the Twenty-First Century: Proceedings of the Congress of the United Nations Commission on International Trade Law* (United Nations, New York, 1992)

## TEXTS

R Balkin and J Davis *Law of Torts* (Butterworths, Sydney, 1991)

A Brown and A Grant *The Law of Intellectual Property in New Zealand* (Butterworths, Wellington, 1989)

JF Burrows, J Finn and S Todd *Law of Contract in New Zealand* (8 ed, Butterworths, Wellington, 1992)

JF Burrows, J Finn and S Todd *Law of Contract in New Zealand* (8 ed, Butterworths, Wellington, 1997)

D Campbell (ed) *Serving Process and Obtaining Evidence Abroad* (Kluwer Law International, London, 1998)

L Clarke *Confidentiality and the Law* (Lloyd's of London Press Ltd, London, 1990)

J Cleary *The Laws of New Zealand: Auction* (Butterworths, Wellington, 1992)

D Denning *Information Warfare and Security* (ACM Press, New York, 1999)

A Fitzgerald et al (eds) *Going Digital: Legal Issues for Electronic Commerce, Multimedia and the Internet* (Prospect Media, St Leonard, NSW, 1998)

C Grice *The Laws of New Zealand: Consumer Protection* (Butterworths, Wellington, 1992) Vol 7

C Gringras *The Laws of the Internet* (Butterworths, London, 1997)

Hon A Grove *The Laws of New Zealand: Consumer Credit and Hire Purchase* (Butterworths, Wellington, 1992) Vol 7

F Gurry *Breach of Confidence* (Clarendon Press, Oxford, 1984)

Halsbury's Laws of England (4 ed, Butterworths, London, 1989) Vol 9(1) Contract

Rt Hon Justice McKay *The Laws of New Zealand: Defamation* (Butterworths, Wellington, 1992)

New Zealand Bankers' Association *Code of Banking Practice* (Wellington, November, 1996)

New Zealand Stock Exchange Fact Book (1998) at <http://www.nzse.co.nz>

P Spiller *Butterworths New Zealand Law Dictionary* (Butterworths, Wellington, 1995)

ICF Spry *The Principles of Equitable Remedies: Specific Performance, Injunctions, Rectification and Equitable Damages* (5 ed, LBC Information Services, Sydney, 1997)

Statistics New Zealand *New Zealand Official Yearbook 1998* (GP Publications, Wellington, 1998)

R Susskind *The Future of Law* (Clarendon Press, Oxford, 1998)

S Todd (ed) *The Law of Torts in New Zealand* (2 ed, Brookers, Wellington, 1997)

## ARTICLES

R Abeyratne "Actions on the Internet of Airline Tickets" (1999) 4(1) Communications Law 22

"Australia-United States Joint Venture on Electronic Commerce" (1998) 5 (21) Electronic Commerce Report 3

"Australian E-Commerce Legislation Goes to Final Drafting" (1999) 6(4) Electronic Commerce Report 5

"Australian Government in About-Turn on Privacy Legislation" (1999) 5(22) Electronic Commerce Report 3

L Barnard "Choice of Law in International Contracts – The Objective Proper Law Reconsidered" (1996) 2(1) NZBLQ 27

G Bastin "Protection of Property in Confidential Information by Employers" (1990) 134(11) Solicitors Journal 307

S Bell "National Office on the Information Economy" *The Independent*, 7 July 1999, 23.

S Bell "NZ Post Targets E-Commerce Top Spot" *The Independent*, 3 October 1997, 23

A Boss "Electronic Commerce and the Symbiotic Relationship Between International and Domestic Law Reform" (1998) 72(6) Tulane Law Review 1931

A Brown "Intellectual and Industrial Property" [1995] New Zealand Law Review 78

K Brown "APEC on ecommerce" *LawTalk* 524, 2 August 1999, 11

R Brownsword and G Howells "When Surfers Start to Shop: Internet Commerce and Contract Law" (1999) 19 Legal Studies 287

S Burbank "The United States' Approach to International Civil Litigation: Recent Developments in Forum Selection" (1998) 19(1) University of Pennsylvania Journal of International Economic Law 1

G Chen "Electronic Commerce on the Internet: Legal Developments in Taiwan" [1997] XVI Journal of Computer and Information Law 77

C Counts and A Martin "Libel in Cyberspace: A Framework for Addressing Liability and Jurisdictional Issues in this New Frontier" (1996) 59 Alb L Rev 1083

"Courts will Sit in Session on the Internet" *The Times*, 11 September 1998, at <http://www.sunday_times.co.uk>

A Davies "How Many Auditors Does It Take to Sign a Report?" *The Independent*, 25 November 1998, 35

M De Zwart "Electronic Commerce: Promises, Problems and Proposals" (1998) 21(2) UNSW Law Journal 305

J Dickie "When and Where are Electronic Contracts Concluded?" (1998) 49(3) Northern Ireland Legal Quarterly 332

W Dodge "Extraterritoriality and Conflict-of-Laws Theory: An Argument for Judicial Unilateralism" (1998) 39(1) Harvard International Law Journal 101

M Donahey "Dispute Resolution in Cyberspace" (1998) 15(4) Journal of International Arbitration 127

D Dorward "The *Forum Non Conveniens* Doctrine and the Judicial Protection of Multinational Corporations from Forum Shopping Plaintiffs" (1998) 19(1) University of Pennsylvania Journal of International Economic Law 141

D Dugdale "Formal Requirements: the Proposed Repeal of the New Zealand Contracts Enforcement Act 1956" (1998) 13 Journal of Contract Law 268

S Dutson "Choice of Law in Tort in Domestic and International Litigation" (1998) 26 Australian Business Law Review 238

C Elliot "The Internet – A New World Without Frontiers" [1998] NZLJ 405

G Evans and B Fitzgerald "Information Transactions Under UCC Article 2B: The Ascendancy of Freedom of Contract in the Digital Millennium?" (1998) 21(2) UNSW Law Journal 404

G Fisher "The International Sales Convention: Scope, Interpretation and Related Matters" *ALTA Conference Proceedings* (Australasian Law Teachers' Association, Dunedin, 1998) Vol 2, 411

B Fitzgerald "Computer Software: Sales, Licences and Consumer Protection" (The 1999 Fay, Richwhite Conference, Auckland, 15–16 July 1999)

G Fitzgerald and L Gamertsfelder "Protecting Informational Products (Including Databases) Through Unjust Enrichment Law: An Australian Perspective" [1998] EIPR 244

S Flower "When Does Internet Activity Establish the Minimum Contact Necessary to Confer Personal Jurisdiction?" (1997) 62 Missouri Law Review 845

C Freedman "Protecting Confidential Commercial Information Through Criminal Law: Comments on Issues" (1999) 4(3) Communications Law 87

J Gailey and J Sibbald "Scottish Courts Online" (June/July 1999, Bristol, United Kingdom) Computers and the Law 3

J Gatson "Standing on Its Head: The Problem of Future Claimants in Mass Tort Class Actions" (1998) 77 Texas Law Review 215

C Gill "Forum Conveniens: the Dilemma after *Berezovsky v Forbes*" (1999) 4(1) Communications Law 16

J Goldsmith "Against Cyberanarchy" [1998] The University of Chicago Law Review 1199

G Greenleaf and others *Commerce on the Internet: The Legal Implications of the Internet* (Wellington and Auckland, Butterworths and the New Zealand Law Society, 1998)

K Griggs "Cold War protocol risks e-commerce" *National Business Review*, 12 February 1999, 6

RG Hammond "The Misappropriation of Commercial Information in the Computer Age" (1986) 64 Canadian Bar Review 342

J Harris "Jurisdiction Clauses and Void Contracts" (1998) 23 EL Rev 279

R Hill "The Internet, Electronic Commerce and Dispute Resolution: Comments" [1997] Journal of International Arbitration 103

"Hope Fading for Uniform Australian E-Commerce Laws" (1999) 6(2) Electronic Commerce Report 3

R Howland, "UNCITRAL Model Law on Electronic Commerce" (1997) 32(6) European Transport Law 703

T Hunter "If you want to get ahead, get online: investors embrace Internet trading" *The Independent*, 14 July 1999, 24

Inland Revenue Department "Guidelines to Taxation and the Internet" 10 August 1999 at <http://www.ird.govt.nz/resource/taxaint/index.htm>

F Juenger "A Hague Judgments Convention?" (1998) 24 Brooklyn Journal of International Law 111

F Juenger "Two European Conflicts Conventions" (1998) 28 VUWLR 527

C Kessedjian *International Jurisdiction and Foreign Judgments in Civil and Commercial Matters* Hague Conference on Private International Law Enforcement of Judgments Prel Doc No 7 (April 1997) at <http://www.state.gov/www/global/legal_affairs/intl_jurisdiction.html>

C Kessedjian "First Impressions of the Transnational Rules of Civil Procedure" (1998) 33(3) Texas International Law Journal 477

Hon Justice Michael Kirby "Privacy in Cyberspace" (1998) 21(2) UNSW Law Journal 323

B Lip "Minor's Civil Law Capacity to Contract on the Internet". Submission to the Queensland Law Reform Commission at <http://www.jcu.edu.au>

E Loh "Intellectual Property: Breach of Confidence?" (1995) 17(8) EIPR 405

E Longworth *Possibilities of a Legal Framework for Cyberspace – Including a New Zealand Perspective* (GP Publications, Wellington, 1999)

Lord Chancellor's Department *Resolving and Avoiding Disputes in the Information Age: A Lord Chancellor's Department Consultation Paper* (September 1998) at <http://www.open.gov.uk/lcd/consult/itstrat/civindex.htm>

F MacMillan "Corporate Disclose On-Line" (1998) 21(2) UNSWLJ 514

D Marshall "Discovery in the Information Age" [1998] Solicitors Journal 856

D McCarty "Internet Contacts and Forum Notice: A Formula For Personal Jurisdiction" (1998) 39(2) William and Mary Law Review 557

P Millett "Tracing the Proceeds of Fraud" (1991) 107 LQR 71

P Myburgh "Bits, Bytes and Bills of Lading: EDI and New Zealand Maritime Law" [1993] NZLJ 324

C Nicoll "Should Computers be Trusted? Hearsay and Authentication with Special Reference to Electronic Commerce" [1999] JBL 332

P Niehaus "Cyberlibel: Workable Liability Standards?" [1996] U Chi Legal F 617

"NOIE deputy chief to head up new National Electronic Authentication Council" 13(6) Electronic Commerce Report 4

"NZSE FASTER system operational" (1999) 499 LawTalk 6

"On-line Auctions E-Commerce Flavour of the Month" (1998) 6(8) Electronic Commerce Report 6

M O'Rourke "Fencing Cyberspace: Drawing Borders in a Virtual World" (1998) 82(3) Minnesota Law Review 609

K O'Shea and K Skeahan "Acceptance of Offers by E-mail – How Far Should the Postal Acceptance Rule Extend?" (1997) 13 QUTLJ 257

T Pullar-Strecker "Government Anti-Piracy Regulations 'Minimal'" *NZ InfoTech Weekly, The Dominion*, 29 August 1999, 4

T Pullar-Strecker "Multiple Currencies for Exporters" *NZ Infotech Weekly, The Dominion*, 25 April 1999, 1

O Renault "Jurisdiction and the Internet – Are Traditional Rules Enough?" (1998) Uniform Law Conference of Canada at <http://www.law.ualberta.ca/alri/ulc/current/ejurisd.htm>

C Rose "The Several Futures of Property: Of Cyberspace and Folk Tales, Emission Trades and Ecosystems" (1998) 83 Minnesota Law Review 129

G Shapira "UNCITRAL and its work – Harmonisation and Unification of International Trade Law" [1992] NZLR 309

M Sneddon "Legislating to Facilitate Electronic Signatures and Records: Exceptions, Standards and the Impact of the Statute Book" (1998) 21(2) U NSWLJ 334

M Solimine "The Quiet Revolution in Personal Jurisdiction" (1998) 73(1) Tulane Law Review 1

Rt Hon Spigelman CJ *Use of Technology in Civil Litigation (Practice Note)* (May 1999) 45 (2) NSWLR v–xi.

B Stewart "Information Security – Privacy Law and Issues" (1997) 2 HRLP 225

R Susskind "How to Court the IT Revolution" *The Times*, London, United Kingdom, 31 August 1999, 21

R Trow "Young NZ Retailers Blocked from Net Payment Service" *NZ Infotech Weekly, The Dominion*, 1 August 1999, 3

D Tyler "Personal Jurisdiction Via E-Mail: Has Personal Jurisdiction Changed in the Wake of *CompuServe Inc v Patterson*?" (1998) 51 Arkansas Law Review 429

"United States Announce Official Agreement on Electronic Commerce" (1998) 5 (21) Electronic Commerce Report 2

A Vanderlaan "*Compuserve Inc v Patterson*: Civil Procedure Enters the Cyber-Age" (1997) 47(4) Saint Louis University Law Journal 1399

D Vick, L Macpherson and S Cooper "Universities, Defamation and the Internet" (1999) 62 The Modern Law Review 58

"Victoria to get E-Commerce and Data Privacy Laws this Year?" (1999) 6(5) Electronic Commerce Report 4

"Web no site for Arthur Daley" *The New Zealand Herald*, 5 May 1999 at <http://www.herald.co.nz>

S Welling and A Rickman "Cyberlaundering: The Risks, The Responses" (1998) 50(2) Fla L Rev 295

A Wells "IBM's shark set to hook into data management" *NZ Infotech Weekly, The Dominion*, 1 August 1999, 7

C Weston "Suing in Tort for Loss of Computer Data" [1999] CLJ 67

S Wheeldon "Reflections on the Concept of 'Property' with Particular Reference to Breach of Confidence" (1997) 8(2) Auck U LR 353

M Whincop and M Keyes "Putting the 'Private' Back Into Private International Law: Default Rules and the Proper Law of the Contract" (1997) 21 Melb U LR 21 515

"Y2K Panel Won't Quit at 2000" *International Herald Tribune*, 15 September 1999, 3

## CASES


*Anns v Merton London Borough Council* [1978] AC 728

*Boardman v Phipps* [1967] 2 AC 46

*Corinthian Pharmaceutical Systems Inc v Lederle Laboratories* (1989) 724 F Supp 605 (SD Ind)

*Cubby Inc v Compuserve Inc* (1991) 776 F Supp 135 (SDNY)

*Daniels v Thompson* [1998] 3 NZLR 22 (CA); on appeal *W v W* [1999] 2 NZLR 1

*Deta Nominees Pty Ltd v Viscount Plastics Pty Ltd* [1979] VR 167

*Dickson Livestock Associates Ltd v Wrightson Ltd* (28 April 1999) unreported, High Court, Wellington, CP 225/97

*Exchange Telegraph v Gregory* [1896] 1 QB 147

*Francome v Mirror Group Newspapers Ltd* [1984] 2 All ER 408

*Franklin v Giddens* [1978] 1 Qd R 72

*Godfrey v Demon Internet Ltd* [1999] 4 All ER 342

*Goldsbro v Walker* [1993] 1 NZLR 394

*Hawkins v Young Hunter* (1997) 10 PRNZ 453

*Heller v Bianco* 244 P 2d 757 (Cal Dist Ct App 1952)

*Henderson v Merretts Syndicates Ltd* [1995] 2 AC 145

*Henthorn v Fraser* [1892] 2 Ch 27

*Inset Systems Inc v Instruction Set Inc* (1996) 937 F Supp 161 (D Conn)

*Invercargill City Council v Hamlin* (1994) 7 PRNZ 674

*Lancashire County Council v Municipal Insurance Ltd* [1996] 2 All ER 545

*Linda Chih Ling Koo, John Ho Hung Chiu v Law Tai Hing* CA Civ App No 116 of 1992, 25 August 1993

*MAI Systems Corporation v Peak Computer Inc* (1993) 991 F 2d 511 (9th Cir)

*Malone v Metropolitan Police Commissioner* [1979] Ch 344

*Merkur Island Shipping Corporation v Laughton* [1983] 2 All ER 189

*Morrow & Benjamin Ltd v Whittington* [1989] 3 NZLR 122

*National Australia Finance Ltd v Tolra* (26 January 1993) unreported, High Court, Wellington, CP735/92

*NBA v Motorola Inc* (1997) 105 F 3d 841 (2d Cir)

*Neumegen v Neumegen & Co* [1998] 3 NZLR 310

*New Zealand Post v Leng* (1998) 8 TCLR 502

*Oggi Advertising Ltd v McKenzie & Ors* [1999] 1 NZLR 631

*Powerbeat International Ltd v Attorney-General* (17 June 1999) unreported, High Court, Hamilton, CP 72/98

*R v Raynes* (10 November 1998) unreported, High Court, Auckland, AP No 86/98

*R v Wilkinson* [1999] 1 NZLR 403

*Ross Industries (New Zealand) Ltd v Talleys Fisheries Ltd and Oths* (5 September 1997) unreported, High Court, Auckland, CP 68/97

*Simpson v Attorney-General (Baigent's Case)* [1994] 3 NZLR 667

*Society of Lloyd's & Oxford Members' Agency Ltd v Hyslop* [1993] 3 NZLR 135

*South Pacific Manufacturing Co Ltd v New Zealand Security Consultants Ltd* [1992] 2 NZLR 282

*Steel Blast & Painters Limited v City Wise Developments Limited* (1995) 3 NZ ConvC 95-256

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

*The Laptop Co Ltd v ANZ Banking Group (New Zealand) Ltd* (1999) 6 NZBLC 102, 833, 99-474

*Thornton v Shoe Lane Parking Ltd* [1971] 2 QB 163

*Van Camp Chocolates Ltd v Aulsebrooks Ltd* [1984] 1 NZLR 354

*Wellington Newspapers Limited v Dealers Guide Ltd* [1984] 2 NZLR 66

*Wilson v New Brighton Panelbeaters Ltd* [1989] 1 NZLR 74

*Woolwich Equitable Building Society v Inland Revenue Commissioners* [1993] AC 71

## UNPUBLISHED

Commission of the European Communities "Proposal for a European Parliament and Council Directive on Certain Legal Aspects of Electronic Commerce in the Internal Market" COM (1998) 586 final 98/0325 (COD) Brussels, 18 November 1998

E-Commerce Business Policy "Main Guiding Principles", 1998 at http://www.ec.gov.sg/sum3_08Apr98.html

Ministry of Foreign Affairs and Trade *New Zealand's Controls on the Export of Strategic Goods* (Wellington, November 1996)

C Nicoll "Insurance of E-Commerce Risks" 1999

OECD Guidelines for Cryptography Policy (March 1997) at <www.oecd.org//dsti/sti/it/secur/prod/e-crypto.htm>

J Song *Electronic Commerce Law – A Review on the Principles in New Zealand Law Commission's Report, Electronic Commerce Part One: NZLC R50* Directed Study Final Report (University of Waikato, 1999)

# Index

References are to paragraphs in the main text of the report unless marked E (Executive Summary)

## 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 (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 |
| NZLC R54 | Computer Misuse (1999) |
| NZLC R55 | Evidence (1999) |
| NZLC R56 | Annual Report (1999) |
| NZLC R57 | Retirement Villages (1999) |

## *Study Paper series*

| | |
|---|---|
| NZLC SP1 | Women's Access to Legal Services |
| NZLC SP2 | Priority Debts in the Distribution of Insolvent Estates: An Advisory Report to the Ministry of Commerce (1999) |

## *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 J H Farrar and M A 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) (1997) |
| 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 (1999) |
| NZLC PP38 | Adoption: Options for Reform (1999) |