E 31AO

Report 54

COMPUTER MISUSE

May 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 1–877187–32-1
This report may be cited as: NZLC R54
Also published as Parliamentary Paper E 31AO

Summary of contents

Contents

13 May 1999

Dear Minister

I am pleased to submit to you Report 54 of the Law Commission, *Computer Misuse*.

Yours sincerely

The Hon Justice Baragwanath
President

The Hon Tony Ryall MP
Minister of Justice
Parliament Buildings
Wellington

Preface

CASES OF COMPUTER MISUSE in New Zealand have recently received much public attention. There have been justified calls for more effective criminal legislation. As an adjunct to its *Electronic Commerce* project, the Law Commission decided late last year to consider how our laws should deal with computer misuse.

In December 1998 the Commission published a short report suggesting an amendment to the Crimes Act 1961 to address the specific problem exposed by the judgment of the Court of Appeal in *R v Wilkinson* [1999] 1 NZLR 403: see *Dishonestly Procuring Valuable Benefits* (NZLC R51 1998). That report also suggested a wider review of Part X of the Crimes Act 1961 (see paras 11-13). The present report deals generally with computer misuse.

The Commission has concluded that the existing criminal law is inadequate. There is plain need for legislative amendment to create specific offences to address various types of computer misuse. Our views are set out briefly in the Executive Summary and in more detail in the body of the report.

The Ministry of Justice has also been considering issues arising out of computer misuse. The Minister for Justice recently announced his proposal to introduce into the House of Representatives legislation which will create criminal offences for certain types of computer misuse (see *New Zealand InfoTech Weekly* 11 April 1999, 1). On 19 April 1999 the Commission supplied to the Ministry of Justice a draft copy of this report so that it could be considered when preparing advice to the Minister.

Originally, we intended to issue this report as a preliminary paper to seek submissions on the views we express. However, because of the imminence of a Bill, we have issued a final report which is confined to concepts and which does not include draft legislation. While we would have preferred more time to consider the form of the legislative changes we consider it important for our work to be available both to the Ministry and the public in time for it to be of use. For comparative purposes we have set out in Appendix A the provisions recommended for New Zealand by the Crimes Consultative Committee in 1991 and examples of provisions to be found in other countries.

This report addresses distinct issues from those raised in the Commission's report *Dishonestly Procuring Valuable Benefits* (NZLC R51 1998), which discusses the Court of Appeal decision *R v Wilkinson* [1999] 1 NZLR 403. We adhere to our recommendation that the solutions recommended in paras 9 and 10 of NZLC R51 be adopted as a matter of urgency.

The Law Commission has been greatly assisted in preparing this report by its Electronic Commerce Advisory Committee. The Commission wishes to express its thanks to the members of that Committee, namely: 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, University of Otago.

The Commissioner in charge of preparation of this report is D F Dugdale. Paul Heath QC, a consultant to the Commission on commercial law issues, has been responsible for overseeing preparation of the report. The research for the report has been undertaken by Jason Clapham to whom the Commission expresses its appreciation.

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

Executive Summary

E1 THERE IS PUBLIC INTEREST in encouraging the use of computers and appropriate standards for users of computers. Criminal sanctions should be available to enforce those standards. Computers allow information to be processed, recorded and transferred quickly and efficiently. It is necessary both to facilitate the use of computer technology (including the removal of barriers to its use) and to provide strong sanctions against reprehensible conduct which, if unchecked, is likely to inhibit use of computer technology.

E2 The Minister of Justice proposes to introduce a Bill into the House of Representatives concerning computer misuse (see *New Zealand InfoTech Weekly*, 11 April 1999, 1). Consequently, draft legislation is not included in this report. This report sets out the reasons for the Commission's view that new legislation is needed and explains the nature of the legislation which is thought to be necessary.

E3 It is preferable to enact a comprehensive law dealing with computer misuse rather than to amend, in a piecemeal fashion, legislation currently in existence.

E4 Legislation dealing with computer misuse must address the following elements:

- Unauthorised interception of data stored[1] in a computer;
- Unauthorised accessing of data stored in a computer;
- Unauthorised use of data stored in a computer;
- Unauthorised damaging of data stored in a computer.

The report explains the types of conduct which fall within each of the concepts listed in paragraph E4.[2]

E5 There are peculiar problems arising from computer misuse. Some forms of misuse will cause loss to the person or persons entitled to the data; others may not. Likewise, some forms of misuse may or

---

[1] The term "stored" is intended to cover both data retained on a computer for any period of time and data which passes through a computer but is not necessarily retained for any period of time. Unless the context requires otherwise, the term "stored" is to be read in that way throughout this report.

[2] See paras 12 –23.

may not enable the person concerned to gain a pecuniary benefit at the expense of the person entitled to the data. It is therefore necessary to express any new law in such a way as to encompass the whole continuum of misuse and leave a wide range of sentencing options available. The court can then determine an appropriate sentence in the light of the facts proved in the particular case.

E6 The offences of unauthorised access and interception should require proof by the prosecution of intent:

- in relation to the interception offence, the prosecution should be required to establish an intention to intercept:
- in relation to the offence of access, the prosecution should be required to establish an intention to:
  - cause loss or harm to the person entitled to the data or to some third party; or
  - gain some form of benefit or advantage either personally or to a third party.

We propose that the terms "loss or harm" and "benefit or advantage" be given a wide meaning and not be limited to pecuniary losses or benefits (see further, para 13). In the case of offences involving use and damage, proof of carelessness should be sufficient to establish an offence.

E7 Our report is presented in the following way:

- Chapter 1 provides an introduction to the subject. This includes a brief summary of the provisions of the existing criminal law which are relevant to computer misuse issues.
- Chapter 2 explains the nature of each of the elements identified in para E4 above with a view to discussing later in the report whether changes are needed to the existing criminal law and, if so, the form which those changes should take.
- Chapter 3 addresses specifically the questions whether the existing criminal law is adequate or whether something more is needed to deal with the problems created by computer misuse.
- Questions of jurisdiction are discussed in chapter 4.
- Recommendations are set out in chapter 5.

E8 There are three Appendices to this report. Appendix A sets out the provisions recommended by the Crimes Consultative Committee in 1991 and legislation to be found in other jurisdictions dealing with similar issues. Appendix B contains a glossary of some technical terms mentioned in this report. Appendix C reproduces chapter 4 of our report *Electronic Commerce Part One: A Guide for the Legal and Business Community* (NZLC R50 1998) which will

enable the reader to consider the issues which arise in relation to the law of torts and the criminal law.

1
Introduction

1 THE USE OF COMPUTERS in society has become widespread. As the Law Commission noted in *Electronic Commerce: Part One* (NZLC R50 1998) business-to-business (as opposed to business-to-consumer) commerce over the Internet[3] reached an estimated US$8 billion in 1997. This was 10 times the 1996 total. The Law Commission also noted that by the year 2002 an estimated US$327 billion will be spent on business-to-business commerce over the Internet. Approximately 10 percent of major New Zealand organisations expect to spend more than $500,000 each in setting up electronic systems in the next two years (para 5). The National Business Review recently reported that, according to Intel, electronic commerce will be worth US$1 trillion by 2002 (NBR, February 26 1999, 55).

2 As at 1 September 1995 there were no company domain names registered on the Internet in New Zealand, yet by the beginning of 1998 there were over 14,000. The New Zealand world wide web domains increased from just under 4,000 as at 1 February 1997 to nearly 9,000 in March 1998 (See *Oggi Advertising Ltd v McKenzie* [1999] 1 NZLR 631; (1998) 6 NZBLC 102,567; (1998) 8 TCLR 36).

---

[3] The Internet was developed by the United States Defence Department in the early 1970s. It was then known as ARPANET (Advanced Research Projects Agency Network). It was designed to provide communications which would not be disrupted even in the event of a major emergency. Computers were interconnected so that each computer in the network was connected to each other computer. Electronic messages could be sent from A to B directly or via any other computer or computers in the network. If part of the network became unoperational, the message would arrive at its destination regardless via an alternative route. The second feature is that the messages are not sent as a single stream of data. Rather they are divided into discrete "packets" that are sent separately and reassembled by the recipient computer. Each packet may take a different route to the destination in order to avoid congestion. The Internet is identical to the ARPANET in its operation with the major difference being that while the ARPANET consisted of approximately 40 computers, there are now literally millions of interconnected computers any of which can communicate freely with the others. The term "Intranet" means an internal network which uses the same technology as the world wide web to show and link documents. It is not necessarily linked to the Internet itself, but when it is it can allow in viruses and hackers from outside (Gringras 1997 3 383).

It has been estimated that as many as 40 million people around the world were using the Internet in 1997 and that this figure would rise to 200 million by 1999 (Gripman, 1997).

3 The issue of extending the criminal law to deter computer misuse has recently assumed prominence both in New Zealand and overseas. In the late 1980s several countries investigated the need for the creation of criminal offences specifically directed at computer misuse. The Scottish Law Commission (*Report on Computer Misuse* (Scot Law Com, No 106) 1987) the Attorney-General's Department of Australia (*Review of Commonwealth Criminal Law: Interim Report, Computer Crime*, November 1988) and the Law Commission of England and Wales (*Criminal Law: Computer Misuse* (Law Com. No 186) 1989) recommended the adoption of criminal offences directed at computer misuse. These recommendations prompted new legislation in the United Kingdom and Australia making computer misuse a criminal offence. Legislation has also been passed in Canada and Singapore relating to computer misuse (see Appendix A where this legislation is reproduced). Also, the South African Law Commission is currently considering issues in relation to computer related crime (see South African Law Commission, *Computer Related Crime*, Issue Paper 14, August 1998).

4 In New Zealand, the Crimes Bill 1989 proposed the creation of two offences in relation to computer misuse; accessing a computer for a dishonest purpose and damaging or interfering with a computer system. The Crimes Consultative Committee completed its report on the Crimes Bill in April 1991 (The Crimes Consultative Committee, *Crimes Bill 1989, Report of the Crimes Consultative Committee* (April, 1991)). The Committee proposed a number of changes to the clauses relating to computer misuse recommending that there should be three separate offences dealing with computer misuse; accessing a computer and obtaining a benefit or causing a loss, accessing a computer with intent to obtain a benefit or cause a loss, and a summary offence of unauthorised access to a computer punishable by a maximum of 6 months imprisonment (75–77).

5 The Crimes Bill 1989 was never enacted. Therefore, New Zealand has no criminal offence aimed squarely at computer misuse. Nevertheless, there are a number of statutory provisions within our criminal law which would address some of the computer misuse issues we have raised. For example:

- Interception of private communications[4] are dealt with in ss 312B–312Q Crimes Act 1961, ss 10 and 18 of the International

[4] Generally, "private communications" is defined as being "oral communications".

Terrorism (Emergency Powers) Act 1987, and ss 14 –28 of the Misuse of Drugs Act 1978.

- So far as gaining access to electronic data is concerned, s 248 of the Crimes Act 1961 relates to impersonation and therefore covers part of the continuum involving access to electronic data.
- Use of electronic data is currently dealt with by provisions relating to theft (s 220 Crimes Act 1961) although, as we pointed out in *Dishonestly Procuring Valuable Benefits* (NZLC R51 1998) there is a lacuna in the law in relation to theft of an intangible thing such as a chose in action. Section 218 of the Crimes Act 1961 deals with theft of electricity. Section 264 of the Crimes Act 1961 (with a restrictive definition of the term "document" contained in s 263 of the same Act) deals with forgery of documents. Finally, there are the general fraud provisions contained in s 229A of the Crimes Act 1961.
- Fraudulent alteration or destruction of the document may be covered by ss 231 and 266A of the Crimes Act 1961. The offence of willful damage under s 298 (4) of the Crimes Act 1961 may also be relevant.

6 We discuss later in this report whether the existing law is sufficient to deal with computer misuse problems and, if not, what type of solution may be preferable.

2
Defining our terms

GENERAL

7 The Crimes Consultative Committee 1991 report recommended three distinct offences (see para 4). Advances in technology since 1991 have revealed additional problems which can properly be characterised as computer misuse.

8 It is important to bear in mind the purpose of the criminal law when deciding whether it is appropriate to provide criminal sanctions for such activities. Sir Carleton Allen stated:

> Crime is crime because it consists in wrongdoing which directly and in serious degree threatens the security or well-being of society, and because it is not safe to leave it redressable only by compensation of the party injured (Smith & Hogan 1992 16).

9 The types of computer misuse identified in paras 24–29 of this report can be characterised as wrongdoing which directly, and to a serious degree, threatens the security or wellbeing of our society which is increasingly reliant on computers to process, record and transfer information for the purposes of both business and social services. There is a need to deter people who may otherwise be inclined to engage in computer misuse and to punish those who do. In that context we address the continuum of conduct which we believe should be encompassed within any criminal law dealing with computer misuse.

10 After consultation with members of our Advisory Committee, we have formed the view that there are four distinct elements with which any criminal law concerning computer misuse must deal. These elements are unauthorised:

- interception of data stored on a computer;
- accessing of data stored on a computer;
- use of data stored on a computer; and
- damaging of data stored on a computer.

We now explain the type of conduct which we intend the terms set out in para 10 to cover.

Explanation as to Use of Technical Terms

11 Various types of conduct should be encompassed within the category of unauthorised interception, access, use and damage of electronic data. We propose to use terms conveyed to us by the technical members of our Advisory Committee which, we are told, are commonly understood by those who use computers and are sufficiently proficient to engage in computer misuse. These terms will, obviously, require translation into a form of language which can be included in a statute should our recommendations be accepted.

Unauthorised

12 The term "unauthorised" is intended to mean: without the express or implied consent of the person entitled to control access to the data. We intend the term "implied consent" to mean consent inferred from proved words or conduct. By defining the term in that way:

- those who access the information with express or implied consent (for instance, computer repairers); or
- those who access the information for a lawful purpose (for example, law enforcement officials executing search warrants)

will not be caught by the criminal law.

Intent

13 We consider that the offence of unauthorised access should require an intent:

- to cause loss or harm to the person entitled to the data or to some third party; or
- to gain some form of benefit or advantage either personally or to a third party.

In our view, an intent to cause loss or harm, or an intent to gain a benefit or advantage is needed to avoid trivialising the criminal law by making every unauthorised access a criminal offence. The requirement of such an intent will mean that those who gain access simply to achieve the prize of access will not be criminally liable for their actions. As we have not suggested that a similar intent be required for the offence of damage (see paras 22, 23 and 93), a person who obtains unauthorised access without an intent to cause loss or harm or to gain a benefit or advantage will still be liable for the offence of "damaging" if damage is caused through careless conduct. We are also of the view that the terms "loss or harm" and "benefit or advantage" need to be given wide meanings so

that they relate to both potential and actual, loss, harm, benefit or advantage. They should also extend to losses and benefits which go beyond pecuniary ones.

Data

14 The word "data" is intended to include all types of information stored on a computer, including the programmes which run the computer as well as personal information.

Computer

15 We have considered how best to define the term "computer". We note that the Attorney-General's Department of Australia, the Law Commission of England and Wales and the Scottish Law Commission (in their reports in relation to computer misuse) all recommended against defining the term "computer". We note that:

- First, computer technology is advancing rapidly and any definition would quickly become obsolete. In that regard the likelihood of technological obsolescence creates an added incentive to avoid technological or media specific language in any statute dealing with computer misuse.
- Secondly, any legal definition of "computer" is likely to be complex and will probably produce extensive argument about the true meaning of the words used.

For these reasons we are of the view that it is best not to define the term. We intend that the term be interpreted in a wide sense so as to include any future technology of similar kind not yet in existence.

Computer Misuse

16 The term "computer misuse" is technology-neutral. The definition does not refer to any particular method of communication. Also, the definition does not limit "computer misuse" solely to land based or long range activities. The definition we have proposed covers both the situation where an individual gains access to a computer from a distance as well as the situation where a person accesses a computer by making physical contact with the computer.

Interception

17 The first category of misuse is the unauthorised *interception* of electronic data. 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.

18 Examples of unauthorised interception of electronic data include:

- *communication channel interruption and pass through* – where the channel is physically breached and the attacker siphons off (or records) data and passes it back to the channel so that the data can continue to the original destination. The receiver would normally be unaware of this type of interception;
- *diverting a transmission via a duplicate channel* –physically splitting the signal so that two or more copies are being transmitted simultaneously, one to the original destination and one to the attacker;
- *packet sniffing* – 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;
- *scanning* – probing of network ports to ascertain the state of each port. The state of any given port is in indication of whether that port might be an avenue of successful entry or attack. Sample tools for accomplishing this are SATAN (Security Audit Tool for Auditing Networks) and ISS (Internet Security Scanner). There are many other tools freely available on the Internet;
- *electromagnetic emanations* – surreptitiously gaining emanations via an induction coil, radio receiver or other device and translating them into usable forms.

Access

19 The second category of misuse is the unauthorised *accessing* of data stored in a computer. This is where a person without authority, whether through physical or electronic means, accesses data stored on a computer. Examples of this are:

- *masquerading* – identity theft (impersonation), document and message forging. This includes all situations in which impersonation or forgery of data occurs;
- *password cracking* – attacking systems and guessing passwords or gaining access to password files and analysing them to derive valid passwords to gain unauthorised entry to a system;
- *spoofing* – forging packet addresses so that the message appears to have originated from a "trusted" source;
- *use of valid passwords* – using another's password to gain unauthorised entry to a system;

- *employee access* – where an employee gains unauthorised access to information.

Use[5]

20 The third category of misuse is the unauthorised *use* of data stored in a computer. The term "use" covers 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. 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. We see the term "use" as covering both *intellectual* uses of data as well as *physical* uses.

21 In the context of the criminal law, we consider that fine distinctions should not be drawn between the use of information which is properly regarded as intellectual property and information which is not currently regarded as property. Later, we suggest (in para 36) that information may need to be redefined generally as a property right for both civil and criminal law purposes. In the context of the criminal law, we are of the view that such fine distinctions are undesirable in principle and will create uncertainty in practice. For that reason, we recommend that any computer misuse statute be worded specifically to over-rule the effect of *Malone v. Metropolitan Police Commissioner (No 2)* [1979] 1 Ch 344, which held that no duty of confidence attaches to information acquired by interception of a telephone conversation. We will address the question whether the civil law should regard information as a property right in our second *Electronic Commerce* report (see, generally, *Electronic Commerce Part One*: at paras 158 –166, attached as Appendix C).

Damage

22 The final category of misuse is *damaging* data stored on a computer. "Damage" is intended to cover the entire continuum from denial of data through to modification of data stored in a computer through to destruction of that data. Given that continuum, it is clear that some types of damage (eg alteration or deletion of data) could be carried out both with and without authority. It is not proposed to criminalise authorised conduct. Further, the term is

[5] There is some case law on the meaning of "use" in the context of privacy and data protection laws (see *R v Brown* [1996] 2 Cr. App. R. 72, H.L. (E.)).

not intended to be limited to permanent damage and would include temporary damage to computer data. This category covers both the "direct" and the "indirect" damaging of data. Examples of "direct" damaging of data are:

- "hacking" into a computer and deleting data;
- adding a "virus", a "worm", a "trojan horse" or a "logic bomb" to a computer system (see Appendix B for definitions of these terms); and
- using an electromagnetic or high energy radio frequency to destroy data stored on a computer.

23 Examples of "indirect" damaging of data are:

- 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;
- entering a password or otherwise blocking legitimate users from being able to access data;[6] and
- denial of service attacks where a person sends many messages at an Internet Service Provider blocking any other transmissions from getting through.

The second and third points are examples of what we have termed "denial of data" in this report.

---

[6] In *Revlon Inc v Logisticon Inc* 705933 (Cal. Super. Ct., Santa Clara City. Complaint filed Oct 22, 1990) a software company dialled into Revlon's computer system and intentionally disabled Revlon's system because Revlon had not paid the software company for certain software. Revlon could not distribute its products as its computer system was disabled for three days losing an estimated $20 million dollars in revenue. The case was settled out of court (cited in Gringras (1997, 170)).

3
Are changes to the criminal law needed?

IS COMPUTER MISUSE A PROBLEM?

24 HAVING EXPLAINED WHAT WE MEAN by the term "computer misuse", the next issue to be considered is whether computer misuse is a problem which deserves the attention of the criminal law. In our view, the answer is plainly "yes",[7] although the extent of the problem is often concealed. Often computer misuse will go undetected. In some situations, a company may decide, for publicity reasons, not to disclose that it has been subject to computer misuse.[8] In the New Zealand context, companies may not report incidents of computer misuse as New Zealand currently does not have criminal offences dealing specifically with such conduct. Also, it may be perceived that the criminal offences which currently exist are inadequate to deal with computer misuse.[9]

25 Recently in New Zealand there have been two widely publicised incidents involving computer misuse. In November 1998, a computer hacker erased some 4,500 "Ihug" websites.[10] The Ihug server was

[7] See http://www.cert.org/ (site of the Computer Emergency Response Team located at Carnegie Mellon University in Pennsylvania); http://www.auscert.org.au (site of the Australian Computer Emergency Response Team located at University of Queensland in Brisbane) and http://ciac.llnl.gov (site of the Computer Incident Advisory Capability, a part of the U.S. Department of Energy located at Lawrence Livermore National Laboratories in Livermore, California) where computer viruses and incidents of computer misuse on the Internet are discussed.

[8] It is noted by Gripman that only 17 percent of respondents who suffered a "hacker" intrusion reported the incident to law enforcement officials. Over 70 percent of the respondents who suffered a hacking intrusion cited negative publicity as the reason for non-disclosure (1997 175).

[9] In the "Ihug" case, discussed at para 25, it was reported that Ihug were considering extraditing the hacker and prosecuting him in the United States as New Zealand law was "inadequate to deal with cyber-vandalism" (The Dominion, *Teenage hacker faces extradition bid* 21/11/98, 10).

[10] Gringras defines website as "a collection of colourful documents on the World Wide Web. They can be used as an electronic brochure or be more active performing tasks for their viewers, such as searching databases or taking orders . . ." (1997 387–388).

based in California and the sites were hosted by Auckland-based Internet service provider, the Internet Group. There was no backup facility and, unless the owners of the websites made their own copies, the web pages were lost permanently (The Dominion, *Hacker wipes out 4500 Web sites* 19/11/98, 3). Recently it was reported that Telecom, New Zealand's largest Internet service provider, is concerned that hackers might be gaining access to the Internet by using customer's passwords and surfing the Internet at the customers' expense (The Dominion, *Telecom on alert after hacker threat* 24/11/98, 1). Following these incidents, a survey was released which showed that only 45 percent of New Zealand information system managers who responded to the survey were satisfied that their business information was safe from external users (The Dominion, *Survey casts doubt on information security* 25/11/98, 14).

26 Gaining unauthorised access to a computer system is relatively easy (see Gripman 1997). Unauthorised access to computer material is becoming more prevalent, and more serious: in 1995 the United States' General Account Office discovered that hackers using the Internet broke into the US Defence Department's computer more than 160,000 times (Gringras 1997 211). In a 1995 survey of 200 businesses, 95 percent admitted to being victims of computer fraud (Gripman 1997 173).

27 Computer misuse can cause many problems. A computer network may be shut down by a virus, or a company's computer system could be interfered with resulting in the company being unable to distribute its product. In addition to severe business losses, the service, repair and restoration costs caused as a result of computer misuse can be staggering. An organisation which has been subject to a hacker intrusion (or suspects it may have been) will have to go to a great deal of expense to ensure that such an attack does not occur again. This may include conducting an audit of the system and revamping the system's security. In *United States v Morris* 928 F.2d 504, 505–06 (2d Cir. 1991) the damage caused by a virus was in the range of US$96 –186 million based upon the labour costs of eradicating the virus and monitoring the computer systems recovery.

28 Gripman notes that according to federal law enforcement estimates, thieves operating through computers steal more than US$10 billion worth of data in the United States annually, and also that the Senate's Permanent Investigations Sub-committee reported that banks and corporations lost US$800 million from hackers in 1995 (1997 170, 173). A 1996 Information Systems Security survey of 236 security managers and executives concluded that 46 percent of the companies surveyed admitted insider abuse of their computer

system. The losses were dramatic: 22 percent indicated losses between US$50,000.00 and US$200,000.00 and an additional 20 percent indicated losses between US$200,000.00 and US$500,000.00 (Gripman 1997 189).

29 Gripman also notes, and this has been confirmed by the Law Commission's Advisory Committee, that virtually every technique a hacker needs to penetrate corporate computers is currently described on the Internet. There are "hacker" magazines available that provide step by step tips (1997 170). Also, there are many sites on the Internet which give instructions on how to "hack". We have deliberately not referred to these sites to avoid giving them unnecessary publicity. We would invite the Ministry of Justice, as part of its work in this area, to consider whether it is necessary for New Zealand to create offences which will prevent such sites being posted from New Zealand. That is a matter outside the scope of this report.

IS THERE A NEED FOR CRIMINAL OFFENCES DEALING WITH COMPUTER MISUSE?

30 From the information contained in paras 24–29 we are satisfied that computer misuse is a serious problem in today's computer based society. The next issue is whether it is necessary to punish computer misuse with criminal sanctions.

31 The question of tortious liability for computer misuse was addressed in *Electronic Commerce Part One* (NZLC R50 1998). These issues were addressed in the context of a review of the law of torts and its applicability in the electronic environment. In Appendix C we reproduce for ease of reference the whole of chapter 4 of the *Electronic Commerce* report.

32 Civil proceedings in tort take the form of an action for recovery of compensatory damages or other available remedies for injuries or loss caused by the acts or omissions of persons in breach of a right or duty imposed by the law. It is likely that a person who, without authority, intercepts a message containing confidential information or who obtains information by reprehensible means will be made subject to a duty of confidence: see paras 158–166 of the *Electronic Commerce* report reproduced in Appendix C. In this report we restrict consideration of computer misuse issues to the criminal sphere, as the question of civil liability for computer misuse will be addressed in the final report on electronic commerce (*Electronic Commerce: Part 2)*.

33 The Law Commission has considered whether it is necessary to create criminal offences directed specifically at computer misuse

or whether the problem of computer misuse can be adequately dealt with by the civil law. We are satisfied that criminal offences dealing specifically with computer misuse are required. The main arguments in favour of the creation of criminal offences for computer misuse are set out in paras 34–39.

34 There is an essential public interest in the use of computers. The use of computers should be encouraged. Computers allow information to be processed, recorded and transferred quickly and efficiently, and have revolutionised the way people learn, travel, interact and conduct business. Computers are now an accepted part of life in almost all parts of the world. Given the importance of computers in our society today, it is imperative that New Zealand keep pace with the rest of the world in the use of new technology. To give effect to the public interest factors identified, it is necessary both to facilitate the use of computer technology (including the removal of barriers from its use) and to provide strong sanctions against reprehensible conduct which, if unchecked, is likely to inhibit the use of computers.

35 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.

36 It is necessary to protect commercial information which may be of immense value.[11] For many businesses operating in this environment, the information which is stored on their computer system 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

---

[11] The Minister of Information Technology, Hon. Maurice Williamson MP, has recently referred to the onset of the "knowledge economy" in his paper at the New Zealand Law Society Conference (M Williamson, 1999). See also, interview with Hon Max Bradford (Minister of Enterprise and Commerce) on Telstra Business, TVNZ, 14 April 1999, in which Mr Bradford discusses the "knowledge based economy"

information and the *systems* which we are proposing to protect in our recommendations in this report. The question of whether information should be regarded as a property right for civil law purposes will be addressed further in the second Electronic Commerce report to be published later this year.

37 It is desirable that New Zealand law develop in line with global developments and imperatives. Given the trans-border and jurisdictional nature of computer use, New Zealand should bring its legislation into line with other nations with which it has major trading relationships.

38 It is necessary to update our laws to reduce New Zealand's vulnerability to computer misuse, both domestically and internationally. Without such laws in the Internet environment, there is a risk that New Zealand could become a ground for computer hacking experimentation. That risk could inhibit New Zealanders from obtaining lawful access to such information from abroad.

39 The law has a role to play in setting appropriate standards for computer use in general and that of the Internet in particular.

40 The main argument against creating criminal offences in relation to *unauthorised access* to data stored in a computer is that this would create an anomaly in terms of existing criminal law which does not punish unauthorised access to information.[12] Gaining unauthorised access to information is an offence only if, in the process of gaining access to the information, some other specified offence such as trespass or theft is committed. If unauthorised access is gained to information without committing a trespass or theft an offence will generally not have been committed (for example, taking a photograph of a document sitting on another's desk from an adjacent building or reading a document over the shoulder of another passenger in an aeroplane).

41 If gaining unauthorised access to computer data is to be a criminal offence, the person who gains such access will be liable to criminal sanctions whereas the person who gains unauthorised access to *exactly the same information* without using a computer (and without committing a trespass or theft) will not have committed an offence.

---

[12] There is currently a criminal offence in relation to interception of private communications (see para 53). Also, unauthorised use of information will often involve criminal activity (for example fraud or theft). Destruction of information will often involve criminal activity (see the provisions in relation to wilful damage under s298(4) Crimes Act 1961).

42 The Law Commission is of the view that the public interest in encouraging the use of computers and in protecting the community from the misuse of computers outweighs the concern about this anomaly. Moreover there are important differences between unauthorised access to information achieved through the use of a computer, and access to information achieved by other means. These are set out in paras 43–46.

43 Information stored on a computer system will not be protected by physical barriers to access or by the law of trespass or theft, as is information recorded on paper.

44 A person who obtains access to a computer can find in one place vast amounts of information which previously might have been stored in a multitude of locations. The facilities of the computer may be used to search for, select and process specific data at very high speeds.

45 The consequences of unauthorised access, in the digital age, go far beyond what is possible with paper-based or manual systems. Unlike access achieved by other means, where access is achieved by unauthorised computer access, the person who achieves access may use the computer to amend or otherwise use the information. The possible consequences of amending information stored on a computer are wide-ranging and serious. Such conduct could affect the country's economy and the lives of many people. Also, a person who gains unauthorised access to information stored in a computer may be tempted to go on and commit more serious activities such as theft or destruction of data.

46 A knowledge based economy is particularly reliant on information stored on a computer.[13]

47 We are satisfied that there needs to be a powerful deterrent to those who would otherwise engage in computer misuse. We recommend that there should be criminal offences which deal with computer misuse.

IS THE EXISTING CRIMINAL LAW ADEQUATE?

48 We have explained our view that "computer misuse" is made up of four categories of activity: the unauthorised *interception*, *accessing*, *use*, and *damaging of* data stored in a computer. In the following paragraphs we consider whether the existing criminal law is adequate to deal with each of these activities.

[13] See para 36.

INTERCEPTION

49 The first category of computer misuse is unauthorised *interception* of electronic data (see paras 10, 17, 18). Both the Telecommunications Act 1987 and the Crimes Act 1961 deal, in a limited fashion, with the interception of private communications by members of the public.[14]

Telecommunications Act 1987

50 Section 6 Telecommunications Act 1987 provides:

> No person shall, without the agreement of the network operator, connect any additional line, apparatus, or equipment to any part of a network or to any line, apparatus, or equipment connected to any part of a network owned by that operator.

51 Under s20C(1) the High Court may grant an injunction restraining a person from engaging in conduct that constitutes, or would constitute, a contravention of s 6. Under s20D(1) every person who engages in conduct that constitutes a contravention of s 6 is liable, at the suit of any person suffering any loss or damage as a result of that conduct, to damages as if that conduct constituted a tort.

52 In the Law Commission's view, this section is inadequate to deal with the unauthorised interception of electronic data. First, the section requires something to be physically attached to a network. However, it is technically possible to intercept electronic data without having to physically attach anything to a network (for instance, it is possible to pick up electromagnetic emanations from various parts of a computer. This is commonly referred to as TEMPEST (Transient Electro Magnetic Pulse Emanation Standard)).[15] Secondly, the section prohibits attaching equipment to "any part of a network or to any line, apparatus, or equipment connected to any part of a network *owned by that operator*". This section is not clearly drafted. An argument could be made that the "line, apparatus, or equipment" referred to in the section are the lines, apparatus and equipment "owned by that [network] operator", in which case,

---

[14] See ss 312B – 312Q Crimes Act 1961; ss10,18 International Terrorism (Emergency Powers) Act 1987; ss 14–28 Misuse of Drugs Act 1978; and ss4A, 4B, 12A New Zealand Security Intelligence Service Act 1969 in relation to the interception of private communications by law enforcement officials (and see also New Zealand Security Intelligence Service Amendment Bill 1998 and New Zealand Security Intelligence Service Bill (No 2) 1999).

[15] See Wim van Eck, (1985 269–286) and Moller, Phrack Magazine, Vol 4, issue 44 (see http://www.infowar.com/ where the paper is reproduced).

the section would not be contravened if a person attaches an interception device to a computer owed by an individual or a company. Thirdly, a person who contravenes the section is only liable to pay damages to a person who has suffered a loss as a result of the conduct. Often, however, a person may not suffer a loss. For instance, a hacker may obtain a benefit without causing a loss to another.

Crimes Act 1961

53 Section 216B(1) Crimes Act 1961 provides that every one is liable to imprisonment for a term not exceeding two years who intentionally intercepts any "private communication" by means of a "listening device". Every person who discloses a private communication which has been intercepted is liable to two years imprisonment (s216C(1)). "Intercept" includes hear, listen to, record, monitor, or acquire the communication while it is taking place. "Private communication" is defined as meaning any *oral communication* made under circumstances that may reasonably be taken to indicate that any party to the communication desires it to be confidential but does not include a communication occurring in circumstances in which any party ought reasonably to expect that the communication may be intercepted by some other person not having the express or implied consent of any party to do so. "Listening device" means any electronic, mechanical, or electromagnetic instrument, apparatus, equipment, or other device that is used or is capable of being used to intercept a private communication (s216A Crimes Act 1961). Sections 216A and 216B Crimes Act 1961 are limited to "oral communications". The sections do not, therefore, apply to the interception of electronic data.

54 The Law Commission is of the view that the current criminal law is inadequate to deal with the unauthorised interception of electronic data. As discussed above, neither the Telecommunications Act 1987 nor the Crimes Act 1961 adequately covers unauthorised interception of electronic data. Having formed the view that the criminal law is inadequate to deal with unauthorised interception of electronic data, the next issue is: what is the best method of reforming the criminal law? This issue is considered in chapter 5.

ACCESS

55 The second category of computer misuse is unauthorised *access* to electronic data (see paras 10, 19). Section 248 Crimes Act 1961 provides that every person who "personates or represents himself or herself to be any person, living or dead, or the husband, wife, widower, widow, executor, administrator, or any relative of any such

person, with intent to fraudulently obtain, for himself or any other person, possession of or title to any property, or any qualification, certificate, diploma, licence, or benefit" is liable to imprisonment for a term not exceeding 7 years.

56 Section 248 is inadequate to deal with unauthorised computer access. First, in most situations where unauthorised access is gained to a computer it will be doubtful that it could be said the case entails impersonation or representation as another. Examples are where an employee without authority accesses restricted information or where a hacker by-passes a security system and accesses information stored on a computer. Secondly, the section does not cover the case of a person impersonating another with the intention of causing a loss as distinct from acquiring a benefit. Also, the objects which the person must intend to obtain in order to infringe the section are very limited. Applying the *ejusdem generis* canon of statutory interpretation, the term "benefit", as used in s248, would be limited by the words which precede it ("any property, or any qualification, certificate, diploma, licence"). We consider that the criminal law is inadequate to deal with unauthorised computer access and that reform of the law is required.[16]

USE

57 Unauthorised use of data stored on a computer is the third category of computer misuse (see paras 10, 20, 21). In the following paragraphs we consider whether the criminal law, as it currently stands, is able to deal with a number of examples of unauthorised use of computer data.

Theft

58 A hacker may gain unauthorised access to data stored in a computer and use that data to commit theft, for instance, by accessing a bank's computer and transferring funds from a third person's account to their own account or downloading confidential information from a third person's computer. Section 220 Crimes Act 1961

---

[16] Recommendation 148 of the Privacy Commissioner in his review of the Privacy Act 1993 states:

> "there should be an offence provision created concerning any person who intentionally misleads an agency by (a) impersonating the individual concerned; or (b) misrepresenting the existence or nature of authorisation from the individual concerned; in order to make the information available to that person or another person or to have the person's information used, altered or destroyed." (Privacy Commissioner November 1998)

covers theft. However, s220 would not cover theft committed with the aid of a computer.

59 Theft is defined as the "act of fraudulently and without colour of right taking… anything capable of being stolen" (s220 Crimes Act 1961). Section 217 Crimes Act 1961 defines "things capable of being stolen" as being:

> Every inanimate thing whatsoever, and every thing growing out of the earth, which is the property of any person, and either is or may be made movable, is capable of being stolen as soon as it becomes movable, although it is made movable in order to steal it.

60 There cannot be theft under s220 Crimes Act 1961 of an intangible thing. In the recent Court of Appeal case, *R v Wilkinson* [1999] 1 NZLR 403, the Court held that the definition in s217 is confined to choses in possession (ie tangible things) and does not extend to an intangible chose in action such as a credit in a bank account. (For a discussion of *R v Wilkinson* see *Dishonestly Procuring Valuable Benefits* (NZLC R51, 1998)). There cannot be theft of "a chose in action, a debt, a copyright, an idea, or confidential information… or any other incorporeal thing" (Robertson, para 217.05). As the law currently stands, therefore, s220 does not adequately deal with theft committed with the aid of a computer.

61 Section 218 provides that it is an offence fraudulently to abstract, consume, or use any electricity. This section would also be inadequate to deal with computer misuse. In the examples given in para 58, it is not electricity which is stolen but a chose in action and confidential information.

Forgery

62 Forgery is defined as:

> (1) Making a false document, knowing it to be false, with the intent that it shall in any way be used or acted upon as genuine, whether within New Zealand or not, or that some person shall be induced by the belief that it is genuine to do or refrain from doing anything, whether within New Zealand or not.
> (2) For the purposes of this section, the expression "making a false document" includes making any material alteration in a genuine document, whether by addition, insertion, obliteration, erasure, removal, or otherwise (s 264 Crimes Act 1961).

63 Section 264 is inadequate to deal with unauthorised use of data stored in a computer for a number of reasons. The first difficulty is that it is not clear that the word "document" includes data stored on a computer. "Document" is defined for the purpose of s264 as including any "disc" (s263 Crimes Act 1961). In *R v Governor of*

Brixton Prison ex p Levin [1997] QB 65 the Court of Appeal considered the interpretation to be given to the word "instrument" in s8(1) Forgery and Counterfeiting Act 1981 (UK), which definition includes the word "disc". The Court held that "disc":

> …embraces the information stored as well as the medium on which it is stored, just as a document consists both of the paper and the printing on it. (79)

64 It is likely that New Zealand courts would interpret "disc" in s263 Crimes Act 1961 to include data stored on a disc. Even so there are still difficulties with relying on s264 in cases where a hacker has altered data stored in a computer. Given the development of computer technology and the wide array of computer systems currently in use, it may not always be possible to argue that data has been stored on a "disc" in a computer. For instance, we have been advised by our Advisory Committee that often data is only modified in a computers memory and not in permanent storage. The term "false document" is narrowly defined in s263 Crimes Act 1961. Also, in many situations, it may be difficult to prove that a hacker who amended a computer document intended to defraud anyone or intended that the document should be used or acted upon as genuine. Lastly, if the process is wholly automated there is authority which suggests that there is no offence because a machine does not have a state of mind (see *Kennison v Daire* (1985) 38 SASR 404; on appeal (1986) 160 CLR 129, where the appellant was convicted of larceny for withdrawing money from an automatic teller machine (ATM) after he had closed his account and withdrawn the money from it. King CJ noted that "The crime of obtaining money by false pretences requires, in my opinion, the intervention of a human being who is induced by the false pretence to part with money. A machine cannot be deceived by a false pretence or other fraud" (p406)).

Fraud

65 It is also unlikely that s229A Crimes Act 1961 will be an effective deterrent to unauthorised use of data stored in a computer. An offence under s229A is committed when a person, with intent to defraud :

(a) Takes or obtains any document that is capable of being used to obtain any privilege, benefit, pecuniary advantage, or valuable consideration; or

(b) Uses or attempts to use any such document for the purpose of obtaining, for himself or for any other person, any privilege, benefit, pecuniary advantage, or valuable consideration.

66 The difficulty with relying on this section is that it is not clear that the word "document" in s229A includes data stored on a computer. "Document" is defined for forgery offences and includes "discs". However, "document" is not defined for the purposes of s229A. It has consequently been submitted that in the absence of any special extended definition of "document" (such as occurs in s263 Crimes Act 1961 and s3 Evidence Amendment Act (No 2) 1980) data held in an electronic form will not be included (Robertson para 229A.04).

67 The criminal provisions which we have considered above would have only a limited deterrent effect on those who would otherwise engage in unauthorised use of data stored on a computer. We consider how best to reform the criminal law to deal with the unauthorised use of computer data in chapter 5.

DAMAGING

68 The final category of computer misuse is the unauthorised damaging of computer data (paras 10, 22, 23). In the following paras we consider whether the existing criminal law is adequate to deal with such activities.

Altering a document

69 Altering a document with intent to defraud occurs where a person "makes any alteration in any document, whether by addition, insertion, deletion, obliteration, erasure, removal, or otherwise" with intent to defraud (s266A Crimes Act 1961). This section could be used, for instance, where a hacker enters a competitor's computer and amends or deletes valuable information.

70 There are a number of difficulties with relying on this section to deter unauthorised damaging of data stored on a computer. As with forgery, it is unclear whether "document" in s266A includes data stored on a computer. Also, s266A will only cover a limited range of conduct. The section will not cover a hacker who alters a document and causes loss to another but cannot be shown to have had an intention to defraud (for example, where the hacker carelessly alters data). In any event, conduct which results in denial of data will not be covered by these provisions.

Fraudulent destruction of a document

71 A computer hacker may gain unauthorised access to confidential data stored on a competitor's computer and delete that information. It will be difficult to prosecute a hacker successfully for such actions

under s266A (see paras 69, 70). It will also be difficult to prosecute a hacker under s231 Crimes Act 1961. Section 231 provides:

> Every one who destroys, cancels, conceals, or obliterates any document for any fraudulent purpose is liable to the same punishment as if he had stolen the document, or to imprisonment for a term not exceeding 3 years, whichever is the greater.

72 There are a number of difficulties with relying on s231 to deter unauthorised damaging of computer data. First, it is not clear that "document" in s231 includes data stored on a computer. Secondly, for there to be a successful prosecution under s231 the prosecution must establish, beyond reasonable doubt, that the hacker acted for a "fraudulent purpose".[17] In many cases this will be difficult to establish. For example, a hacker may attempt to gain access to data stored in a computer simply as a test of personal computer expertise. In the process of doing this the hacker might, carelessly, destroy data stored in the computer. In such a case, it would be unlikely that the court would find that the hacker had acted with a "fraudulent purpose". Thirdly, if a hacker was successfully prosecuted under s231 for fraudulently damaging data stored in a computer, the maximum penalty that could be imposed would be three years imprisonment (as we have seen, it is not possible to "steal" data contained on a computer; paras 59–60).

Wilful Damage

73 Under s298(4) Crimes Act 1961 it is an offence punishable by up to 5 years imprisonment to "wilfully destroy" or "damage" any "property". A person will have acted "wilfully" if she/he acted "recklessly".[18]

74 It is likely that a computer hacker will be guilty of an offence of wilful damage under s298 if he or she wilfully or recklessly damages data in a computer. "Property" will most likely include information stored on a computer. The definition of "property" in the Crimes Act 1961 includes intangible property ("any debt, and any thing in action, and any other right or interest" (s2)). Also, two English cases under section 1(1) Criminal Damage Act 1971 (UK) have

---

[17] "Fraudulent purpose" is not defined in the Crimes Act 1961. However, it has been held that the deliberate destruction of documents to conceal improper or dishonest conduct will amount to a "fraudulent purpose" (***R v Shea*** (13/8/97, CA221/97)).

[18] Section 293 Crimes Act 1961 provides:

> … every one who causes any event by an act which he knew would probably cause it, being reckless whether that event happens or not, shall be deemed to have caused it wilfully.

resulted in convictions for computer misuse, that section is similar to s298(4) Crimes Act 1961 (see para 75). The material difference between the two Acts is that in the UK Act "property" is confined to property of a *tangible* nature (s10(1)).

75 In *Cox v Riley* (1986) 83 Cr App R 54, the defendant had deliberately erased a computer programme from a plastic circuit card of a computerised saw so as to render the saw inoperable. It was held that the computer card was "property" and that the defendant had damaged the card as the card could not operate the saw until it had been re-programmed which would require time, effort and money. In *R v Whiteley* (1991) 93 Cr App R 25, the defendant had gained access to a computer network and had altered data contained on discs in the system. Evidence was given that the discs were so constructed as to contain upon them magnetic particles. The Crown's case was that the defendant had caused damage to the discs by altering the state of the magnetic particles on the discs so as to delete and add files. The Court of Appeal held that the defendant had been rightly convicted. The Lord Chief Justice stated:

> There can be no doubt that the magnetic particles upon the metal discs were part of the discs and if the appellant was proved to have intentionally and without lawful excuse altered the particles in such a way as to cause an impairment of the value or usefulness of the disc to the owner, there would be damage within the meaning of section 1. (28–29)

76 There are however two difficulties with relying on s298 to deter unauthorised destruction of computer data.

77 First, it appears that "damage" in s298 is confined to the situation where there has been *lasting* damage. "Damage" is not defined in the Crimes Act 1961. In *Kathness v Police* (Auckland HC, 31 October 1983, M 1291/83, Barker J), a case of wilful damage under s11 Summary Offences Act 1981,[19] Barker J quoted with apparent approval the definition of "damage" given in *Police v Consedine and Gillooly* (1981) 1 D.C.R 267. In that case "damage" was defined as meaning "to do or cause damage to [or] to injure (a thing) so as to lessen or destroy its value. . . physical injury to a thing such as impairs its value or usefulness" (2). In *Kathness* it was held that spray painting a road had "damaged" the road as the spray painting

---

[19] Section 11 Summary Offences Act 1981 provides:

(1) Every person is liable to imprisonment for a term not exceeding 3 months or a fine not exceeding [$2,000] who intentionally–(a) Damages any property …

had impaired the road's value. The Judge stated that $47 had to be spent to restore the road to its original condition.

78 In *Cox v Riley*, *R v Whiteley* and *Kathness* there was a physical alteration to property which impaired the property's value and which required work to return the property to its original state. Where there is only a temporary functional derangement of a computer (and then the computer is restored to its original condition) it would be difficult to argue that the computer had been "damaged" within the meaning of the Act. A temporary interruption of some computers could have serious consequences, for instance, a temporary interruption of an airport control system or a computer in a hospital.

79 Secondly, it is not clear that s298 would cover the "indirect" destruction of computer data such as the examples discussed at para 23**.** To be an effective deterrent against the unauthorised destruction of computer data, the Crimes Act 1961 needs to make it clear that "indirect" destruction is covered as well as direct destruction.

80 We conclude that the existing criminal law is inadequate to deal with computer misuse. However, it would be possible to redraft existing law to cover the types of computer misuse to which we have referred in this report. If an attempt is made to amend the existing provisions of the Crimes Act 1961 to make them fit the matters discussed in this paper, there is a grave risk of error either by imposing criminal liability where it should not be imposed or by omitting provisions that ought to be included. We have no doubt that the only neat and sensible solution is to either have a separate statute dedicated to crimes of computer misuse, or, to have a distinct part within the Crimes Act 1961 relating to computer misuse. Accordingly, in chapter 5 we proceed to make recommendations on the framework for a criminal law dealing with computer misuse.

4
Jurisdiction

81 The English Court of Appeal has recently considered the issue of jurisdiction in a case involving international computer misuse. In *R v Governor of Brixton Prison ex p Levin* [1997] QB 65 the applicant accessed a US bank computer from Russia in order to transfer funds to his own account. The English Court of Appeal held that acts necessary to constitute the offences of forgery and theft had been committed in the US. In relation to forgery, the Court stated:

> The applicant's keyboard was connected electronically with the Citibank computer in…[the US]; as he pressed the keys his actions, as he intended, recorded or stored information for all practical purposes simultaneously on the magnetic disk in the [US] computer. That is where the instrument was created and where the act constituting the offence was done (80).

82 The Court went on to state:

> In the case of a virtually instantaneous instruction intended to take effect where the computer is situated it seems to us artificial to regard the insertion of an instruction onto the disk as having been done only at the remote place where the keyboard is situated (82).

83 In New Zealand, courts will have jurisdiction in respect of offences under the Crimes Act 1961 if:

> any act or omission forming part of any offence, or any event necessary to the completion of any offence occurs within New Zealand…whether the person charged with the offence was in New Zealand or not at the time of the act, omission, or event (s 7 Crimes Act 1961).

84 There is no New Zealand authority which considers the issue of jurisdiction in a case of international computer misuse. However, it is likely that New Zealand courts will assume jurisdiction where a person situated overseas commits an offence involving a computer in New Zealand. In *Solicitor-General v Reid* [1997] 3 NZLR 617 the respondent had sworn a false affidavit in New Zealand for use in proceedings in the Hong Kong Court of Appeal in return for NZ$1million. Justice Paterson stated that had he been required to determine the issue he would have held that New Zealand courts

had jurisdiction to hear the case. Justice Paterson expressed approval of the decision in *Libman v The Queen* (1985) 21 CCC (3d) 206 where the Supreme Court of Canada held that the test was whether there was a "real and substantial link" between the offence and the country asserting jurisdiction to try the offence. He also held that there was nothing contrary to international comity in such an assumption of jurisdiction. Justice Paterson stated:

> In this case, all the activities which constituted the attempt to pervert the course of justice took place in New Zealand. The affidavit was sworn here and the one million dollars was paid here. There was a real and substantial link between the offence under s 117(d) of the Crimes Act [obstructing the course of justice] and New Zealand. International comity in this case suggests that New Zealand should have jurisdiction as it is contrary to good international relations to stand by and allow events to occur in New Zealand which harm the judicial process in another country. There is certainly nothing in international comity which suggests that Mr Reid should not be prosecuted here. For these reasons, I would have held that the court did have jurisdiction to convict Mr Reid (632).

85 It is probable that New Zealand courts would follow the approach taken in *R v Governor of Brixton Prison ex p Levin* and in *Solicitor-General v Reid*. Assuming this is correct, New Zealand courts would generally assume jurisdiction where either the computer or the hacker were situated in New Zealand.

86 However, in our view the existing jurisdiction provisions in the Crimes Act 1961 are inadequate to deal with computer misuse activities. First, there are situations where the effects of computer misuse may be felt in New Zealand even though neither the hacker nor the computer were situated in this country.[20] In these situations, it may not always be possible to successfully argue, in terms of s 7 Crimes Act 1961, that "any act or omission forming part of [the] offence, or any event necessary to the completion of [the] offence" had occurred within New Zealand. Secondly, in many cases it will be impossible to determine where the hacker was at the time the computer misuse activities took place.

---

[20] For instance, the hacker may be in New York, the computer in California and the owner of the computer system in New Zealand. For example, in the "Ihug" case discussed at para 25 the computer was based in California and was owned by a New Zealand company.

87 Computer misuse is international and can be committed across borders with ease. Given this fact, as well as the difficulties of relying on the current jurisdiction provisions of the Crimes Act 1961, we recommend that a provision be enacted giving New Zealand courts jurisdiction in computer misuse offences wherever they are committed.[21]

---

[21] A number of statutory provisions give New Zealand courts jurisdiction in relation to offences committed outside New Zealand. For instance, s144A Crimes Act 1961 provides that it is an offence for a New Zealand citizen to do any act to any child under the age of 16 years outside New Zealand, if that act would, if done in New Zealand, constitute an offence.

5
Recommendations

88 We are of the view that new offences dealing specifically with computer misuse should be created and that such offences should be located in a separate statute or in a distinct part of the Crimes Act 1961. We hold this view for the following reasons:

- it will enable a comprehensive code to be readily available to legal practitioners and to the public. This is a preferable approach to that which would involve practitioners and members of the public scouring various statutes to see whether any offence was likely to be, or had been, committed;
- computer related activities can be dealt with by legislation expressed in suitable (but preferably technologically neutral) language;
- the criminal law in relation to computer misuse would be rendered clear and certain. At present, we do not believe that the existing criminal law can adequately deal with all forms of computer misuse.

89 In the Law Commission's view there should be four new offences dealing with computer misuse. These are set out in paras 90–93.

90 *Unauthorised interception of data stored in a computer*:[22] To prove this offence the prosecution should be required to show; first, that the accused obtained unauthorised interception of computer data, and secondly that the accused *intentionally* intercepted the computer data. Those who accidentally intercept computer data should not be subject to prosecution under the section. The offence should also be expressed so as to include instances where the hacker physically attaches an interception device to a computer or transmission device (such as telephone wires) as well as instances where the hacker places a device in proximity to such equipment

[22] The terms "data" and "unauthorised" are intended to convey the meanings set out in paras 12–14. The term "computer" should not be defined for the reasons given in para 15.

(see para 18 where electromagnetic emanations are discussed). If it was thought necessary to define the term "interception device" it may be appropriate to use the definition of "listening device" in s216A Crimes Act 1961 (as discussed in para 53).

91 *Unauthorised access to data stored in a computer*: This offence should be expressed in the manner specified in para 13. It is not appropriate to punish with criminal sanctions a person who accidentally or 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. 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.

92 *Unauthorised use of data stored on a computer*: This offence should be expressed so as to cover both:

- those who have gained access to data stored in a computer and then go on to "use" that data (see paras 20 and 21); and
- those who receive and use data without authority (see paras 20 and 21).

As to the first, a hacker should be liable for unauthorised use irrespective of how access to the data was gained (whether intentionally or unintentionally). As to the second, a person who receives data from a person knowing that that person has obtained it through unauthorised means should also be liable for criminal sanctions.

93 *Unauthorised damaging of data stored in a computer*: This offence should cover the entire continuum from denial of data to complete destruction of data. It would be sufficient to prove that the hacker gained unauthorised access and that data was damaged as a result of the hacker's actions (whether intentional or careless). This will ensure that those who gain unauthorised access without an intent to cause loss or harm or to derive some benefit or advantage, will be liable for the offence of damaging data whether the damage was caused deliberately or carelessly. It would also be sufficient that the defendant, without gaining access to the computer programme at all, nevertheless damaged data (see para 22 third bullet point).

94 We recommend that there be a single maximum penalty set for all four categories of computer misuse activity. It would then be for the court to exercise a discretion when sentencing depending

on the gravity of the particular case. A case could involve a person intentionally gaining access to a computer system operated by a national security or law enforcement agency with major damage occurring through a careless or reckless act. Accordingly, we believe that the maximum penalty must be set at a high level. We would suggest a period of 10 years imprisonment. The court can reflect appropriate penalties to fit the circumstances of particular cases within that maximum limit.

95 We also recommend that the new legislation should expressly give New Zealand courts jurisdiction in international computer misuse cases in the manner set out in para 87.

APPENDIX A
Legislation

SUMMARY:

96 APPENDIX A IS IN TWO PARTS. In the first part of the Appendix the legislation from a number of jurisdictions is summarised. In the second part, the actual legislation is reproduced.

United Kingdom

97 In 1990 the United Kingdom enacted the Computer Misuse Act 1990 (UK). The Computer Misuse Act 1990 (UK) substantially implemented the recommendations contained in the English Law Commission's report of 1989. Under section 1 it is an offence to cause a computer to perform any function for the purpose of securing unauthorised access to a computer and the person knows that such access is unauthorised. A person will be guilty of an offence under section 2 if they obtain unauthorised access to a computer (under section 1) with intent to commit or to facilitate the commission of another offence. A person will be guilty of an offence under section 3 if he or she does an act which causes an unauthorised modification of the contents of a computer. The person must know that any modification he or she intends to achieve is unauthorised.

98 The Computer Misuse Act 1990 (UK) also addresses jurisdiction in cases where the computer hacking is international (See s 4(2)).

Australia

99 Australia has a number of statutes which create computer related crimes. There is legislation at both the Commonwealth and the state levels.

100 At the Commonwealth level, Part VIA of the Crimes Act 1914 creates a number of offences in relation to computer misuse. The offences contained in the Crimes Act 1914 substantially mirror the recommendations made in the 1988 interim report of the Australian Attorney General's Department. Under the Crimes Act 1914 it is an offence to:

- intentionally obtain unauthorised access to a Commonwealth computer;
- obtain unauthorised access to a Commonwealth computer with intent to defraud any person;
- intentionally obtain unauthorised access to certain types of confidential data; and
- intentionally destroy or interfere with data stored in a Commonwealth computer (sections 76A–76F Crimes Act 1914).

101 Most of the states and territories in Australia have legislation dealing with computer misuse.[23] In the Australian Capital Territory and New South Wales offences of intentionally gaining unauthorised access to a computer (s309(1) Crimes Act 1900 (NSW), s135J Crimes Act 1900 (ACT)); accessing a computer with intent to obtain a benefit or to cause a loss (s309 Crimes Act 1900 (NSW); s135L Crimes Act 1900 (ACT)); and intentionally destroying, altering or interfering with a computer (s135K Crimes Act 1900 (ACT); s310 Crimes Act 1900 (NSW)) have been created. The New South Wales Act provides a higher penalty if a hacker gains unauthorised access to certain types of confidential information stored in a computer (ss309(3), (4) Crimes Act 1900 (NSW)).

Canada

102 Under s 342.1 of the Canadian Criminal Code an offence is committed when a person fraudulently and without colour of right either obtains a "computer service", intercepts a function of a computer system, or uses a computer system to commit such an offence. Giving access to another to enable that other to commit such an offence is also covered. The offence of mischief under s 430(1.1) also covers computer hacking. It is an offence to interfere with "data".

Singapore

103 Singapore has also introduced legislation to deal with computer misuse. The Computer Misuse Act 1993 (Sing.) is similar to the Computer Misuse Act 1990 (UK). However, under s6(1)(a) of the Singapore Act it is an offence to gain unauthorised access to a computer for the purpose of obtaining a "computer service". "Computer service" is defined as including "computer time, data processing

[23] See ss135H–135L Crimes Act 1900 (ACT); ss 308–310A Crimes Act 1900 (NSW); ss 222, 223, 276 Criminal Code Act (REPCO33)(NT); Summary Offences Act 1953 (SA); ss 257–257F Criminal Code 1924 (Tas); s408D Criminal Code 1899 (Qld); s440A Criminal Code Act Compilation Act 1913 (WA).

and the storage or retrieval of data" (s2). It is also an offence under s6 to intercept (which includes to listen to or to record) any computer function (s6(1)(b)). Unlike the United Kingdom Act therefore, the Singapore Act makes it an offence to eavesdrop on a computer.

LEGISLATION:

New Zealand

Crimes Bill 1989:

199 Interpretation –

For the purposes of this section and of sections 200 and 201 of this Act:

"Access", in relation to any computer, computer system, or computer network, means instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of the computer, computer system, or computer network.

"Computer" means an electronic device that performs logical, arithmetic, and memory functions by the manipulation of electronic or magnetic impulses; and includes all input, output, processing, storage, software, or communication facilities that are connected or related to such a device in a computer system or a computer network.

"Computer network" means

(a) An interconnection of communication lines with a computer through remote terminals; or

(b) A complex consisting of 2 or more interconnected computers.

"Computer programme" means an instruction or a statement or a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from the computer system.

"Computer software" means a set of computer programmes, procedures, and associated documentation concerned with the operation of a computer system.

"Computer system" means a set of related computer equipment, devices, and software, whether connected or unconnected to one another.

200 Accessing computer system for dishonest purpose

Every person is liable to imprisonment for 7 years who, directly or indirectly–

(a) Accesses any computer, computer system, or computer network, or any part of any computer, computer system, or computer network, with intent to dishonestly obtain for himself or herself or for any other person any privilege, benefit, pecuniary advantage, or valuable consideration; or

(b) Having accessed (whether with or without authority) any computer, computer system, or computer network, dishonestly uses the computer, computer system, or computer network to obtain for himself or herself or for any other person any privilege, benefit, pecuniary advantage, or valuable consideration.

201 Damaging or interfering with computer system–
Every person is liable to imprisonment for 5 years who, having accessed (with or without authority) any computer system, intentionally and without authority damages, deletes, modifies, or otherwise interferes with any data stored in the computer system.

Crimes Consultative Committee's Recommendation (1991):

199 Interpretation–
"Access", in relation to any computer system, means instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of the computer system:
"Computer" means an electronic device that performs logical, arithmetic, and storage functions by the programmed manipulation of electronic, optical, or magnetic impulses or signals, or by a combination of these:
"Computer system" means –
(a) a computer; or
(b) two or more interconnected computers; or
(c) any communication links between computers or to remote terminals; or
(d) both (b) and (c) combined–
together with all related input, output, processing, storage, software,or communication facilities and stored data:
"Software" means a programme, procedure or instruction, or a set of procedures or instructions, together with associated statements and documentation, concerned with the operation of a computer system and designed to enable a computer system to function in the manner required.

200 Accessing computer system for dishonest purpose
Every person is liable to imprisonment for 5 years who, directly or indirectly, accesses any computer system, or any part of any computer system, with intent dishonestly or by deception –
(a) to obtain for himself or herself or any other person any property, privilege, benefit, service, pecuniary advantage, or valuable consideration; or
(b) to cause loss to any other person.

201 Damaging or interfering with computer system
Every person is liable to imprisonment for 5 years who, intentionally or recklessly, and without authority–
(a) Damages, deletes, modifies, or otherwise interferes with any data or software stored in any computer system; or
(b) causes any data or software stored in any computer system to be damaged, deleted, modified or otherwise interfered with.

ENGLAND (COMPUTER MISUSE ACT 1990):

1 Unauthorised access to computer material

(1) A person is guilty of an offence if:
   (a) he causes a computer to perform any function with intent to secure access to any program or data held in a computer;
   (b) the access he intends to secure is unauthorised; or
   (c) he knows at the time when he causes the computer to perform the function that this is the case.

(2) The intent a person has to commit an offence under this section need not be directed at
   (a) any particular program or data;
   (b) a program or data of any particular kind; and
   (c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or both.

2 Unauthorised access with intent to commit or facilitate commission of further offences

(1) A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorised access offence") with intent:
   (a) to commit an offence to which this section applies; or
   (b) to facilitate the commission of such an offence (whether by himself or by any other person) and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

(2) This section applies to offences
   (a) for which the sentence is fixed by law; or
   (b) for which a person of twenty one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or in England and Wales might be so sentenced but for the restrictions imposed by section 33 of the Magistrates Courts Act 1980).

(3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.

(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.

(5) A person guilty of an offence under this section shall be liable:
   (a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or both; and
   (b) on conviction on indictment, to imprisonment for a term not exceeding five years, or to a fine, or both.

3 Unauthorised modification of computer material

(1) A person is guilty of an offence if:

(a) he does any act which causes the unauthorised modification of the contents of any computer; and
(b) at the time when he does the act he has the requisite intent and the requisite knowledge.

(2) For the purposes of subsection (1)b above the requisite intent is an intent to cause a modification of the contents of any computer and by so doing
(a) to impair the operation of any computer;
(b) to prevent or hinder access to any program or data held in any computer; or
(c) to impair the operation of any such program or the reliability of any such data.

(3) The intent need not be directed at:
(a) any particular computer;
(b) any particular program or data or a program or data of any particular kind; or
(c) any particular modification or a modification of any particular kind.

(4) For the purpose of subsection (1)(b) above, the requisite knowledge is knowledge that any modification he intends to cause is unauthorised.

(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary.

(6) For the purposes of the Criminal Damage Act 1971 a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.

(7) A person guilty of an offence under this section shall be liable:
(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or both; and
(b) on conviction on indictment, to imprisonment for a term not exceeding five years, or to a fine, or both.

4 Territorial scope of offences under this act

(1) Except as provided below in this section, it is immaterial for the purposes of any offence under section 1 or 3 above:
(a) whether any act or other event proof of which is required for conviction of the offence occurred in the home country concerned; or
(b) whether the accused was in the home country concerned at the time of any such act or event.

(2) Subject to subsection (3) below, in the case of such an offence at least one significant link with domestic jurisdiction must exist in the circumstances of the case for the offence to be committed.

(4) Subject to section 8 by where
(a) any such link does in fact exist in the case of an offence under section 1 above; and

(b) commission of that offence is alleged in proceedings for an offence under section 2 above;

section 2 above shall apply as if anything the accused intended to do or facilitate in any place outside the home country concerned which would be an offence to which section 2 applies if it took place in the home country concerned were the offence in question.

(5) This section is without prejudice to any jurisdiction exercisable by a court in Scotland apart from this section.

(6) References in this Act to the home country concerned are references –

(a) in the application of this Act to England and Wales, to England and Wales;

(b) in the application of this Act to Scotland, to Scotland; and

(c) in the application of this Act to Northern Ireland, to Northern Ireland.

5 Significant links with domestic jurisdiction

(1) The following provisions of this section apply for the interpretation of section 4 above.

(2) In relation to an offence under section 1, either of the following is a significant link with domestic jurisdiction –

(a) that the accused was in the home country concerned at the time when he did the act which caused the computer to perform the function; or

(b) that any computer containing any program or data to which the accused secured or intended to secure unauthorised access by doing that act was in the home country concerned at that time.

(3) In relation to an offence under section 3, either of the following is a significant link with domestic jurisdiction –

(a) that the accused was in the home country concerned at the time when he did the act which caused the unauthorised modification; or

(b) that the unauthorised modification took place in the home country concerned.

…

8 Relevance of external law

(1) A person is guilty of an offence triable by virtue of section 4(4) above only if what he intended to do or facilitate would involve the commission of an offence under the law in force where the whole or any part of it was intended to take place.

(2) A person is guilty of an offence triable by virtue of section 1(1A) of the Criminal Law Act 1977 only if the pursuit of the agreed course of conduct would at some stage involve:

(a) an act or omission by one or more of the parties; or

(b) the happening of some other event;

constituting an offence under the law in force where the act, omission or other event was intended to take place.

(3) A person is guilty of an offence triable by virtue of section 1(1A) of the Criminal Attempts Act 1981 or by virtue of section 7(4) above only if what he had in view would involve the commission of an offence under the law in force where the whole or any part of it was intended to take place.

(4) Conduct punishable under the law in force in any place is an offence under that law for the purposes of this section, however it is described in that law.

(5) Subject to subsection (7) below, a condition specified in any of subsections (1) to (3) above shall be taken to be satisfied unless not later than rules of court may provide the defence serve on he prosecution a notice:
   (a) stating that, on the facts as alleged with respect to the relevant conduct, the condition is not in their opinion satisfied;
   (b) showing their grounds for that opinion; and
   (c) requiring the prosecution to show that it is satisfied.

(6) In subsection (5) above "the relevant conduct" means:
   (a) where the condition in subsection (1) above is in question, what the accused intended to do or facilitate;
   (b) where the condition in subsection (2) above is in question, the agreed course of conduct; and
   (c) where the condition in subsection (3) above is in question, what the accused had in view.

(7) The court, if it thinks fit, may permit the defence to require the prosecution to show that the condition is satisfied without the prior service of a notice under subsection (5) above.

(8) If by virtue of subsection (7) above a court of solemn jurisdiction in Scotland permits the defence to require the prosecution to show that the condition is satisfied, it shall be competent for the prosecution for that purpose to examine any witness or to put in evidence any production not included in the lists lodged by it.

(9) In the Crown Court the question whether the condition is satisfied shall be decided by the judge alone.

(10) In the High Court of Justiciary and in the sheriff court the question whether the condition is satisfied shall be decided by the judge or, as the case may be, the sheriff alone.

...

Interpretation

(1) The following provisions of this section apply for the interpretation of this Act.

(2) A person secures access to any program or data held in a computer if by causing a computer to perform any function he:
   (a) alters or erases the program or data;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;
(c) uses it; or
(d) has it output from the computer in which it is held (whether by having it displayed or in any other manner);

and references to access to a program or data (and to an intent to secure such access) shall be read accordingly.

(3) For the purposes of subsection (2)(c) above a person uses a program if the function he causes the computer to perform:
(a) causes the programme to be executed; or
(b) is itself a function of the program.

(4) For the purposes of subsection (2)(d) above:
(a) a program is output if the instructions of which it consists are output; and
(b) the form in which any such instructions or any other data is output (and in particular whether or not it represents a form in which, in the case of instructions, they are capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial.

(5) Access of any kind by any person to any program or data held in a computer is unauthorised if:
(a) he is not himself entitled to control access of the kind in question to the program or data; and
(b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled [but this subsection is subject to section 10].

(6) References to any program or data held in a computer include references to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium.

(7) A modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer:
(a) any program or data held in the computer concerned is altered or erased; or
(b) any program or data is added to its contents;

and any act which contributes towards causing such a modification shall be regarded as causing it.

(8) Such a modification is unauthorised if:
(a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and
(b) he does not have consent to the modification from any person who is so entitled.

(9) References to the home country concerned shall be read in accordance with section 4(6) above.

(10) References to a program include references to part of a program.

Commonwealth (Crimes Act 1914)

76A. Interpretation

(1) In this Part, unless the contrary intention appears:

"carrier" means:

(a) a carrier (within the meaning of the Telecommunications Act 1997); or

(b) a carriage service provider (within the meaning of that Act).

"Commonwealth" includes a public authority under the Commonwealth.

"Commonwealth computer" means a computer, a computer system or a part of a computer system, owned, leased or operated by the Commonwealth.

"data" includes information, a computer program or part of a computer program.

(2) In this Part:

(a) a reference to data stored in a computer includes a reference to data entered or copied into the computer; and

(b) a reference to data stored on behalf of the Commonwealth in a computer includes a reference to:

(i) data stored in the computer at the direction or request of the Commonwealth; and

(ii) data supplied by the Commonwealth that is stored in the computer under, or in the course of performing, a contract with the Commonwealth.

76B. Unlawful access to data in Commonwealth and other computers

(1) A person who intentionally and without authority obtains access to:

(a) data stored in a Commonwealth computer; or

(b) data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer;

is guilty of an offence. Penalty: Imprisonment for 6 months.

(2) A person who:

(a) with intent to defraud any person and without authority obtains access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer; or

(b) intentionally and without authority obtains access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer, being data that the person knows or ought reasonably to know relates to:

(i) the security, defence or international relations of Australia;

(ii) the existence or identity of a confidential source of information relating to the enforcement of a criminal law of the Commonwealth or of a State or Territory;

(iii) the enforcement of a law of the Commonwealth or of a State

or Territory;

(iv) the protection of public safety;

(v) the personal affairs of any person;

(vi) trade secrets;

(vii) records of a financial institution; or

(viii) commercial information the disclosure of which could cause advantage or disadvantage to any person;

is guilty of an offence. Penalty: Imprisonment for 2 years.

(3) A person who:

(a) has intentionally and without authority obtained access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer;

(b) after examining part of that data, knows or ought reasonably to know that the part of the data which the person examined relates wholly or partly to any of the matters referred to in paragraph (2)(b); and

(c) continues to examine that data;

is guilty of an offence. Penalty for a contravention of this subsection: Imprisonment for 2 years.

76C. Damaging data in Commonwealth and other computers

A person who intentionally and without authority or lawful excuse:

(a) destroys, erases or alters data stored in, or inserts data into, a Commonwealth computer;

(b) interferes with, or interrupts or obstructs the lawful use of, a Commonwealth computer;

(c) destroys, erases, alters or adds to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer; or

(d) impedes or prevents access to, or impairs the usefulness or effectiveness of, data stored in a Commonwealth computer or data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer;

is guilty of an offence.

Penalty: Imprisonment for 10 years.

76D. Unlawful access to data in Commonwealth and other computers by means of Commonwealth facility

(1) A person who, by means of a facility operated or provided by the Commonwealth or by a carrier, intentionally and without authority obtains access to data stored in a computer, is guilty of an offence. Penalty: Imprisonment for 6 months.

(2) A person who:

(a) by means of a facility operated or provided by the Commonwealth or by a carrier, with intent to defraud any person and without authority obtains access to data stored in a computer; or

(b) by means of such a facility, intentionally and without authority

obtains access to data stored in a computer, being data that the person knows or ought reasonably to know relates to:

(i) the security, defence or international relations of Australia;

(ii) the existence or identity of a confidential source of information relating to the enforcement of a criminal law of the Commonwealth or of a State or Territory;

(iii) the enforcement of a law of the Commonwealth or of a State or Territory;

(iv) the protection of public safety;

(v) the personal affairs of any person;

(vi) trade secrets;

(vii) records of a financial institution; or

(viii) commercial information the disclosure of which could cause advantage or disadvantage to any person;

is guilty of an offence.

Penalty: Imprisonment for 2 years.

(3) A person who:

(a) by means of a facility operated or provided by the Commonwealth or by a carrier, has intentionally and without authority obtained access to data stored in a computer;

(b) after examining part of that data, knows or ought reasonably to know that the part of the data which the person examined relates wholly or partly to any of the matters referred to in paragraph (2)(b); and

(c) continues to examine that data;

is guilty of an offence. Penalty for a contravention of this subsection: Imprisonment for 2 years.

76E. Damaging data in Commonwealth and other computers by means of Commonwealth facility

A person who, by means of a facility operated or provided by the Commonwealth or by a carrier, intentionally and without authority or lawful excuse:

(a) destroys, erases or alters data stored in, or inserts data into, a computer;

(b) interferes with, or interrupts or obstructs the lawful use of, a computer; or

(c) impedes or prevents access to, or impairs the usefulness or effectiveness of, data stored in a computer;

is guilty of an offence. Penalty: Imprisonment for 10 years.

76F. Saving of State and Territory laws

Sections 76D and 76E are not intended to exclude or limit the concurrent operation of any law of a State or Territory.

135H. Interpretation

(1) In this Division, unless the contrary intention appears:
"data" includes information, a computer program or part of a computer program.

(2) A reference in this Division to data stored in a computer includes a reference to data entered or copied into the computer, whether temporarily or permanently.

135J. Unlawful access to data in computer

A person who, intentionally and without lawful authority or excuse, obtains access to data stored in a computer is guilty of an offence punishable, on conviction, by imprisonment for 2 years.

135K. Damaging data in computers

A person who intentionally or recklessly, and without lawful authority or excuse–

(a) destroys, erases or alters data stored in, or inserts data into, a computer; or

(b) interferes with, or interrupts or obstructs the lawful use of, a computer; is guilty of an offence punishable, on conviction, by imprisonment for 10 years.

135L. Dishonest use of computers

(1) A person who, by any means, dishonestly uses, or causes to be used, a computer or other machine, or part of a computer or other machine, with intent to obtain by that use a gain for himself or herself or another person, or to cause by that use a loss to another person, is guilty of an offence punishable, on conviction, by imprisonment for 10 years.

(2) In this section, "machine" means a machine designed to be operated by means of a coin, bank-note, token, disc, tape or any identifying card or article.

New South Wales: (Crimes Act 1900)

308. Definitions

In this Part:

(a) a reference to data includes a reference to information; and

(b) a reference to a program or data includes a reference to part of the program or data; and

(c) a reference to data stored in a computer includes a reference to data entered or copied into the computer.

309. Unlawful access to data in computer

(1) A person who, without authority or lawful excuse, intentionally

obtains access to a program or data stored in a computer is liable, on conviction before two justices, to imprisonment for 6 months, or to a fine of 50 penalty units, or both.

(2) A person who, with intent:
  (a) to defraud any person; or
  (b) to dishonestly obtain for himself or herself or another person any financial advantage of any kind; or
  (c) to dishonestly cause loss or injury to any person,
  (d) obtains access to a program or data stored in a computer is liable to imprisonment for 2 years, or to a fine of 500 penalty units, or both.

(3) A person who, without authority or lawful excuse, intentionally obtains access to a program or data stored in a computer, being a program or data that the person knows or ought reasonably to know relates to:
  (a) confidential government information in relation to security, defence or inter-governmental relations; or
  (b) the existence or identity of any confidential source of information in relation to the enforcement or administration of the law; or
  (c) the enforcement or administration of the criminal law; or
  (d) the maintenance or enforcement of any lawful method or procedure for protecting public safety; or
  (e) the personal affairs of any person (whether living or deceased); or
  (f) trade secrets; or
  (g) records of a financial institution; or
  (h) information (other than trade secrets) that has a commercial value to any person that could be destroyed or diminished if disclosed, is liable to imprisonment for 2 years, or to a fine of 500 penalty units, or both.

(4) A person who:
  (a) without authority or lawful excuse, has intentionally obtained access to a program or data stored in a computer; and
  (b) after examining part of that program or data, knows or ought reasonably to know that the part of the program or data examined relates wholly or partly to any of the matters referred to in subsection (3); and
  (c) continues to examine that program or data,

  is liable to imprisonment for 2 years, or to a fine of 500 penalty units, or both.

(5) A prosecution for an offence under subsection (1) may be commenced at any time within 2 years after the time when the offence is alleged to have been committed.

310. Damaging data in computer

A person who intentionally and without authority or lawful excuse:
  (a) destroys, erases or alters data stored in or inserts data into a computer; or

(b) interferes with, or interrupts or obstructs the lawful use of a computer, is liable to penal servitude for 10 years, or to a fine of 1,000 penalty Units, or both.

Northern Territory: (Criminal Code Act)

222. Unlawfully obtaining confidential information

Any person who unlawfully abstracts any confidential information from any register, document, computer or other repository of information with intent to cause loss to a person or with intent to publish the same to a person who is not lawfully entitled to have or to receive it, or with intent to use it to obtain a benefit or advantage for himself or another, is guilty of a crime and is liable to imprisonment for 3 years.

223. Unlawfully disclosing trade secrets

Any person who unlawfully publishes or discloses a trade secret with intent to cause loss to a person or to obtain a benefit or advantage for himself or another is guilty of a crime and is liable to imprisonment for 3 years.

276. Making false data processing material

(1) Any person who unlawfully alters, falsifies, erases or destroys any data processing material with any fraudulent intention is guilty of a crime and is liable to imprisonment for 3 years.

(2) If he does so with the intent that an incorrect data processing response will be produced and with the intent that it may in any way be used or acted upon as being correct, whether in the Territory or elsewhere, to the prejudice of any person or with intent that any person may, in the belief that it is correct, be induced to do or refrain from doing any act, whether in the Territory or elsewhere, he is liable to imprisonment for 7 years.

South Australia (Summary Offences Act 1953)

44. Unlawful operation of computer system

(1) A person who, without proper authorisation, operates a restricted-access computer system is guilty of an offence.

(2) The penalty for an offence against subsection (1) is as follows:
   (a) if the person who committed the offence did so with the intention of obtaining a benefit from, or causing a detriment to, another-division 7 fine or division 7 imprisonment.
   (b) in any other case-division 7 fine.

(3) A computer system is a restricted-access computer system if:
   (a) the use of a particular code of electronic impulses is necessary in order to obtain access to information stored in the system or operate the system in some other way; and
   (b) the person who is entitled to control the use of the computer system has withheld knowledge of the code, or the means of producing it, from all other persons, or has taken steps to restrict

knowledge of the code, or the means of producing it, to a particular authorised person or class of authorised persons.

Queensland: (Criminal Code Act 1899)

408D. Computer hacking and misuse

(1) A person who uses a restricted computer without the consent of the computer's controller commits an offence.
Maximum penalty: 2 years imprisonment.

(1) If the person causes or intends to cause detriment or damage, or gains or intends to gain a benefit, the person commits a crime and is liable to imprisonment for 5 years.

(2) If the person causes a detriment or damage or obtains a benefit for any person to the value of more than $5 000, or intends to commit an indictable offence, the person commits a crime and is liable to imprisonment for 10 years.

(3) It is a defence to a charge under this section to prove that the use of the restricted computer was authorised, justified or excused by law.

(4) In this section:
"benefit" includes a benefit obtained by or delivered to any person;
"computer" means all or part of a computer, computer system or computer network and includes, for example, all external devices connected to the computer in any way or capable of communicating with each other as part of a system or network.
"controller" means a person who has a right to control the computer's use.
"damage" includes:
(a) damage to any computer hardware or software; and
(b) for information–any alteration, addition, removal or loss of, or other damage to, information.
"information" includes data, file, document, or computer language or coding.
"detriment" includes any detriment, pecuniary or otherwise, to any person.
"restricted computer" means a computer for which:
(a) a device, code or a particular sequence of electronic impulses is necessary in order to gain access to or to use the computer; and
(b) the controller:
(i) withholds or takes steps to withhold access to the device, or knowledge of the code or of the sequence or of the way of producing the code or the sequence, from other persons; or
(ii) restricts access or takes steps to restrict access to the device or knowledge of the code or of the sequence, or to the way of producing the sequence, to a person or a class of person authorised by the controller.
"use", of a restricted computer, includes accessing or altering any information stored in, or communicate information directly or indirectly to or from, the restricted computer, or cause a virus to become

installed on or to otherwise affect, the computer.

Tasmania (Criminal code 1924)

257A. Interpretation:

In this chapter:

"data" includes information, a computer programme or part of a computer programme;

"gain access" includes to communicate with a computer.

257B. Computer-related fraud

A person who, with intent to defraud:

(a) destroys, damages, erases, alters or otherwise manipulates data stored in, or used in connection with, a computer; or

(b) introduces into, or records or stores in, a computer or system of computers by any means data for the purpose of:

(i) destroying, damaging, erasing or altering other data stored in that computer or that system of computers; or

(ii) interfering with, interrupting or obstructing the lawful use of that computer or that system of computers or the data stored in that computer or system of computers; or

(c) otherwise uses a computer.

is guilty of a crime.

257C.Damaging computer data

A person who intentionally and without lawful excuse–

(a) destroys, damages, erases or alters data stored in a computer; or

(b) interferes with, interrupts or obstructs the lawful use of a computer, a system of computers or any part of a system of computers or the data stored in that computer or system of computers–

is guilty of a crime.

257D. Unauthorised access to a computer

A person who, without lawful excuse, intentionally gains access to a computer, system of computers or any part of a system of computers, is guilty of a crime.

257E. Insertion of false information as data

A person who dishonestly introduces into, or records or stores in, a computer or a system of computers, by any means, false or misleading information as data is guilty of a crime.

257F. Extra-territorial application of this chapter

(1) If:

(a) a person does an act or thing referred to in sections 257B to 257E (both inclusive) outside, or partly outside, Tasmania; and

(b) there is a real and substantial link within the meaning of

subsection (2) between doing the act or thing and Tasmania those sections apply in relation that act or thing as if it had been done wholly within Tasmania.

(2) For the purposes of subsection (1), there is a real and substantial link with Tasmania:
   (a) if a significant part of the conduct relating to, or constituting, the doing of the act or thing occurred in Tasmania; or
   (b) where the act or thing was done wholly outside Tasmania or partly within Tasmania, if substantial harmful effects arose in Tasmania.

Western Australia: (The Criminal Code Act Compilation Act 1913)

440A. Unlawful operation of a computer system

(1) In this section:
   (a) "system" means a computer system or a part or application of a computer system;
   (b) a system is a restricted-access system if–
   (i) the use of a particular code, or set of codes, of electronic impulses is necessary in order to obtain access to information stored in the system or operate the system in some other way; and
   (ii) the person who is entitled to control the use of the system has withheld knowledge of the code, or set of codes, or the means of producing it, from all other persons, or has taken steps to restrict knowledge of the code or set of codes, or the means of producing it, to a particular authorised person or class of authorised persons.

(2) A person who without proper authorisation –
   (a)gains access to information stored in a restricted-access system; or
   (b) operates a restricted-access system in some other way
   is guilty of an offence and is liable to imprisonment for one year or a fine of $4,000.00.

(3) A prosecution for an offence under subsection (2) may be commenced at any time.

CANADA (CANADIAN CRIMINAL CODE):

342. (1) Unauthorised use of computer

Every one who, fraudulently and without colour of right,
   (a) obtains, directly or indirectly, any computer service,
   (b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system.
   (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or
   (d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c)

is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

(2) In this section:

"computer password" means any data by which a computer service or computer system is capable of being obtained or used;

"computer program" means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

"computer service" includes data processing and the storage or retrieval of data;

"computer system" means a device that, or a group of interconnected or related devices one or more of which,

(a) contains computer programs or other data, and

(b) pursuant to computer programs,

(i) performs logic and control, and

(ii) may perform any other function;

"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system;

"electro-magnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing;

"function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system;

"intercept" includes listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof.

"traffic" means, in respect of a computer password to traffic, sell, export from or import into Canada, distribute or deal with in any other way.

430 (1.1) Mischief

Every one commits mischief who wilfully:

(a) destroys or alters data;

(b) renders data meaningless, useless or ineffective;

(c) obstructs, interrupts or interferes with the lawful use of data; or

obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.

…

(5) Everyone who commits mischief in relation to data

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or

is guilty of an offence punishable on summary conviction.

…

(8) In this section, "data" has the same meaning as in section 342.1

SINGAPORE (COMPUTER MISUSE ACT 1993):

2. Interpretation:

(1) In this Act, unless the context otherwise requires–

"computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility;

"computer output" or "output" means a statement or representation (whether in written, printed, pictorial, graphical or other form) purporting to be a statement or representation of fact:

(a) produced by a computer; or

(b) accurately translated from a statement or representation so produced;

"computer service" includes computer time, data processing and the storage or retrieval of data;

"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer;

"electronic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer;

"function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer;

"intercept", in relation to a function of a computer, includes listening to or recording a function of a computer, or acquiring the substance, meaning or purport thereof;

"program or computer program" means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function.

(2) For the purposes of this Act, a person secures access to any program or data held in a computer if by causing a computer to perform any function he –

(a) alters or erases the program or data;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) uses it; or

(d) causes it to be output from the computer in which it is held (whether by having it displayed or in any other manner),

and references to access to a program or data (and to an intent to secure such access) shall be read accordingly.

(3) For the purposes of subsection (2)(c), a person uses a program if the function he causes the computer to perform–
   (a) causes the program to be executed; or
   (b) is itself a function of the program.

(4) For the purposes of subsection (2)(d), the form in which any program or data is output (and in particular whether or not it represents a form in which, in the case of a program, it is capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial.

(5) For the purposes of this Act, access of any kind by any person to any program or data held in a computer is unauthorised or done without authority if –
   (a) he is not himself entitled to control access of the kind in question to the program or data; and
   (b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.

(6) A reference in this Act to any program or data held in a computer includes a reference to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium.

(7) For the purposes of this Act, a modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer -
   (a) any program or data held in the computer concerned is altered or erased;
   (b) any program or data is added to its contents; or
   (c) any act which impairs the normal operation of any computer,

and any act which contributes towards causing such a modification shall be regarded as causing it.

(8) Any modification referred to in subsection (7) is unauthorised if –
   (a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and
   (b) he does not have consent to the modification from any person who is so entitled.

(9) A reference in this Act to a program includes a reference to part of a program.

3. Unauthorised access to computer material

(1) Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $2,000.00 or to imprisonment for a term not exceeding 2 years or to both.

(2) If any damage caused by an offence under this section exceeds

$10,000.00, a person convicted of the offence shall be liable to a fine not exceeding $20,000.00 or to imprisonment for a term not exceeding 5 years or to both.

(3) For the purposes of this section, it is immaterial that the Act in question is not directed at:
   (a) any particular program or data;
   (b) a program or data of any kind; or
   (c) a program or data held in any particular computer.

4. Unauthorised access with intent to commit or facilitate commission of further offences

(1) Any person who causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer with intent to commit an offence to which this section applies shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $50,000.00 or to imprisonment for a term not exceeding 10 years or to both.

(2) This section shall apply to offences involving property, fraud, dishonesty or which causes bodily harm punishable on conviction with imprisonment for a term of 2 years or more.

(3) For the purposes of this section, it is immaterial whether the offence to which this section applies is to be committed at the same time when the unauthorised access is secured or on any future occasion.

5. Unauthorised modification of computer material

(1) Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $2,000.00 or to imprisonment for a term not exceeding 2 years or to both.

(2) If any damage caused by an offence under this section exceeds $10,000.00, a person convicted of the offence shall be liable to a fine not exceeding $20,000.00 or to imprisonment for a term not exceeding 5 years or to both.

(3) For the purposes of this section, it is immaterial that the act in question is not directed at:
   (a) any particular program or data;
   (b) a program or data of any kind; or
   (c) a program or data held in any particular computer.

(4) For the purposes of this section, it is immaterial whether an unauthorised modification is, or is intended to be, permanent or merely temporary.

6. Unauthorised use or interception of computer service

(1) Subject to subsection (2), any person who knowingly–
   (a) secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service;
   (b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electromagnetic, acoustic, mechanical or other device; or

(c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b),

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $2,000.00 or to imprisonment for a term not exceeding 2 years or to both.

(2) If any damage caused by an offence under this section exceeds $10,000.00, a person convicted of the offence shall be liable to a fine not exceeding $20,000.00 or to imprisonment for a term not exceeding 5 years or to both.

(3) For the purposes of this section, it is immaterial that the unauthorised access or interception is not directed at –

(a) any particular program or data;

(b) a program or data of any kind; or

a program or data held in any particular computer.

APPENDIX B[25]
Glossary

Disc: a medium for the storage of data. Most disks now in use are magnetically coated, and store the 1's and 0's of digital data by imprinting (or not imprinting) a tiny magnetic field on the disk. Optical disks work on a similar basis with a laser and a reflective (or non-reflective) coating.

Download: to transfer data from a remote (usually large) computer to a local (usually small) one.

Logic bomb: a nasty section of codes which is covertly inserted into a program or operating system. It triggers some activity whenever a specific condition is met. The activity is generally destructive.

Password: A sequence of characters which serves as a kind of text key in gaining access to computers. To maintain security, passwords should be known only to their owners and be hard to guess.

Packet: a way of organising data for communication. Instead of a steady stream of bits and bytes, most computer communications split data into discreet packets. As well as data, each packet typically contains the address to which the packet is being sent, a number which denotes that packet's place in the sequence and information which helps to detect and correct errors. Some packets also contain information about what type of data is being sent. Others serve administrator functions in setting up routes and managing the flow of data. The advantage of packets is their flexibility and efficiency. Packets from different communications can easily be intermixed to maximise use of a line. Packets from the same communication can travel by different routes to speed passage over a crowded network. Given the speed of today's computers, packets can easily carry time-sensitive data, like interactive video, or voice conversations. But the drawback of packet data is, nonetheless, the extra overhead of splitting data into packets at one end and recombining them at the other.

[25] These definitions are drawn from Gringras (1997 379–388)

Trojan horse: a program used to capture unsuspecting people's log-ons and passwords. Typically a Trojan horse looks like the screen ordinarily presented when first logging on to a computer. But, unlike the usual screen, it records the log-on and password - where the creator of the Trojan horse can later retrieve them - before allowing the user to go about his or her business.

Virus: a computer virus is actually a generic term for computer code which replicates, not only throughout the storage medium in which it incubates, but also across the network to which that computer is connected. Without anti-viral software a computer connected to the Internet poses a threat to all other computers also connected, and risks infection from those other computers. The ability to infect a home page with a virus, and even a word processing document, makes the Internet capable of spreading malicious code widely and rapidly.

Worm: a programme that propagates itself across a network, automatically transferring itself to distant machines and running itself there (from whence it transfers itself to more machines). In contrast to a virus which secretes itself inside another program and thus is only spread when the programme carrying it is spread worms take charge of their own reproduction. This reproduction and expansion can cause the computer storage system to run more slowly and can also cause the computer itself to slow down. It is important to note that is does not attach itself to the operating system of the computer it infects; it does not directly impair the workings of a computer.

APPENDIX C
The law of torts

> [T]he law of tort is the general law, out of which the parties can, if they wish, contract; and . . . the same assumption of responsibility may, and frequently does, occur in a contractual context. Approached as a matter of principle, therefore, it is right to attribute to that assumption of responsibility, together with its concomitant reliance, a tortious liability, and then to inquire whether or not that liability is excluded by the contract because the latter is inconsistent with it. (*Henderson v Merrett Syndicates Ltd* [1995] 2 AC 145 (HL), per Lord Goff of Chieveley, 193)

138 THE LAW OF TORTS GOVERNS CIVIL RIGHTS AND DUTIES owed among various members of society. Unlike the law of contract (where obligations are consensual in nature), rights and duties in tort are imposed by law. Sir Ivor Richardson, the current President of our Court of Appeal, recently said:

> [T]he law of torts may be viewed as supplementing contract law by devising rules for allocating or spreading losses in situations where it is too costly for potential injurers and potential victims to enter into contractual relationships with each other to make that allocation. . . . And precedential decisions of the courts in common law jurisdictions may supply a level of detail that is costly to duplicate through private bargaining.[46]

139 Civil proceedings in tort take the form of an action for recovery of compensatory damages or other available remedies for injuries or losses caused by the acts or omissions of another or others in breach of a right or duty imposed by the law.[47]

---

[46] Sir Ivor Richardson, "What can Commercial Lawyers expect of a Legal System?" (8th Inter-Pacific Bar Association Conference, Auckland, 2 May 1998); see also his article "Law and Economics" (1998) 4 NZBLQ 64, 68–71. Compare with Lord Goff of Chieveley in *Henderson v Merrett Syndicates Ltd* (quoted above).

[47] Laws NZ, *Tort*, paras 1–3; see Todd et al 1997 chapter 25 for a general discussion of tortious remedies available in New Zealand.

140 In a commercial context the law of torts is concerned primarily with compensating losses caused to economic interests, whether physical or intangible, when a right is breached or a duty is not adequately performed. Under the Accident Rehabilitation and Insurance Compensation Act 1992 s 14 and its predecessors, it is not generally possible to bring claims for damages arising out of personal injury in New Zealand. This has had an effect on the way in which the law has developed.

141 There is no exhaustive definition of the law of torts. Historically, new torts developed, from time to time, to address social needs arising from the changing nature of society. For example, in *M'Alister (or Donoghue) v Stevenson* [1932] AC 562 (HL) the concept of a duty of care was expanded in a way which addressed the development of (then) modern packaging and distribution methods for consumer goods. Before that the courts had not recognised that a duty to take reasonable care in the manufacturing of products could extend beyond contractual relationships. This was despite the existence of distribution networks involving wholesalers and retailers which did not involve contractual relationships between the manufacturer and the ultimate customer.[48] At the present time new torts seem to be emerging to meet modern society's concerns, for example, invasion of privacy: *Bradley v Wingnut Films Ltd* [1993] 1 NZLR 415; and harassment: *Khorasandjian v Bush* [1993] QB 727.

142 It is perhaps best to start with Lord Atkin's dictum in *M'Alister (or Donoghue) v Stevenson* [1932] AC 562 (HL) in which his Lordship, in discussing the concept of "neighbourhood" for negligence purposes, said:

> The liability for negligence, whether you style it such or treat it as in other systems as a species of "culpa", is no doubt based upon a general public sentiment of moral wrongdoing for which the offender must pay. But acts or omissions which any moral code would censure cannot in a practical world be treated so as to give a right to every person injured by them to demand relief. In this way rules of law arise which limit the range of complainants and the extent of their remedy. The rule that you are to love your neighbour becomes in law, you must not injure your neighbour; and the lawyer's question, Who is my Neighbour? receives a restricted reply. You must take reasonable care to

[48] In this context reference can also be made to further development in New Zealand through the Consumer Guarantees Act 1993.

> avoid acts or omissions which you can reasonably foresee would be likely to injure your neighbour. Who, then, in law is my neighbour? The answer seems to be – persons who are so closely and directly affected by my act that I ought reasonably to have them in contemplation as being so affected when I am directing my mind to the acts or omissions which are called in question. (580)

Those observations of Lord Atkin form the basis of our current law of negligence, even though that law has expanded somewhat to meet changing social and policy requirements (see paras 168–169).

143 In the context of electronic commerce it is relevant to question whether Parliament should seek to impose restrictions upon the operation of the law of torts because of the prospect of exposing persons trading through the internet to "liability in an indeterminate amount for an indeterminate time to an indeterminate class": *Ultramares Corporation v Touche* NY Rep 170, 174 (1931).

144 Examples of the type of issues raised by electronic commerce conducted over the internet are:

- tensions between desires of internet users that all information be freely accessible and the needs of the commercial community to protect intellectual property rights or communications made in confidence;[49]
- potential liability in defamation of internet service providers who act as agents for users of the internet – without internet service providers the information on the internet could not be "published" at all in that form;[50] and
- the potential for damage to be caused to computer systems using the internet through the negligent or intentional spread of computer viruses.[51]

145 The second of our guiding principles proceeds on the premise that fundamental principles underlying the law of torts should not be changed but should be adapted, if necessary, to meet the needs of

---

[49] See the judgment of the United States District Court in *American Civil Liberties Union v Reno* 929 F Supp 824 (1996); affirmed on appeal by the US Supreme Court in *Reno v American Civil Liberties Union* 117 SCt 2329 (1997).

[50] For a recent case dealing with defamation in the context of alleged republication of alleged defamatory material contained on a website see *International Telephone Link Pty Ltd v IDG Communications Ltd* (unreported, HC, Auckland, 20 February 1998, CP344/97).

[51] While there is no case directly in point, a duty not to allow a biological virus, such as foot and mouth disease, to be transmitted has been held to exist: *Weller v Foot & Mouth Disease Research Institute* [1965] 3 All ER 560.

the electronic environment. The question is whether there is any need to adapt the law to take account of technological developments.

146 This chapter considers those torts which are likely to give rise to difficulties in the electronic environment in the context of business-to-business transactions involving international trade. It is necessary to assume that the law to be applied in the international transaction will be the law of New Zealand;[52] accordingly, the law is addressed from that perspective.

TRESPASS TO PROPERTY

147 Trespass to property is a wrongful interference with goods in the possession of another (Todd et al 1997 para 11.2.1). The interference must be direct and physical, but the defendant need not make personal contact with the goods (eg, it is a trespass to goods if damage is caused by use of a projectile: Todd et al para 11.2.2). It is unclear whether the interference with goods may be unintentional, or whether actual damage to the goods must result in order for the elements of the tort to be established: for example, *Wilson v New Brighton Panelbeaters Ltd* [1989] 1 NZLR 74. However, as the usual remedy for trespass to property is damages for the diminution of value or cost of repairing the goods, it is unlikely that a potential plaintiff will commence proceedings unless his or her property has been damaged. In an electronic environment, the main question which arises is whether it is possible to recover in trespass for damage caused by a computer hacker or a computer virus.[53]

148 The question of whether it is possible to claim damages in trespass

---

[52] As a matter of New Zealand domestic law, it is likely that an action in tort will only arise in an international transaction if the alleged tortious act occurred in New Zealand, or the alleged tortious act was committed in a foreign country in which it would also be actionable: *Red Sea Insurance Co Ltd v Bouygues SA* [1994] 3 All ER 749 (PC) 761.

[53] Hacking has been defined as electronic or physical penetration of a computer system by an unauthorised user (Gringras 1997 212); in England and Wales a criminal offence is committed by a "hacker" under the Computer Misuse Act 1990 (see generally Gringras 211–227). A computer virus is a generic term for computer code which replicates, not only throughout the storage medium in which it incubates, but also across the network to which that computer is connected. Without anti-viral software a computer connected to the internet poses a threat to all other computers also connected and risks infection from those other computers. The ability to infect a home page with a virus and even a word processing document makes the internet capable of spreading malicious code widely and rapidly (Gringras 1997 228).

for losses caused by hacking or a computer virus raises three basic issues:

- whether hacking or the introduction of a virus into a computer constitutes interference with goods;
- whether there is any liability in trespass for unintentionally transmitting a virus; and
- the nature of the damage caused.

Interference with goods

149 The tort of trespass to goods requires direct and immediate interference with the plaintiff's goods by the defendant (Todd et al para 11.2.2; Clerk and Lindsell 1995 paras 13-159–13-161). There is no requirement that the defendant physically touch the plaintiff's goods; for example, in *Hamps v Derby* [1948] 2 KB 311 the defendant interfered with the plaintiff's goods (racing pigeons) by shooting at them.

150 Although there appear to have been no cases in which transmission of a computer virus has been held to constitute a trespass to goods, there is a clear analogy between deliberately shooting at personal property with the intention of causing damage to it and deliberately transmitting a computer virus (whether by email or on an infected disc) with the intention of damaging the recipient's computer system. In both cases, the wrongdoer seeks to harm the plaintiff's property by use of a device capable of inflicting damage at a distance.[54] The same result is achieved where a hacker deliberately alters computer files in order to cause inconvenience or damage to the owner.

151 There is authority in English criminal cases that altering a magnetic disc constitutes damage to property: *Nicholas Alan Whiteley* (1991) 93 Cr App Rep 25; *Cox v Riley* (1986) 83 Cr App Rep 54. In *Nicholas Alan Whiteley*, the Court of Appeal stated that where "the interference with the disc amounts to an impairment of the value or usefulness of the disc to the owner, then the necessary damage is established" (29). In doing so Lord Lane CJ distinguished between tangible property being damaged and the damage itself being tangible. The decision suggests that such conduct would constitute wrongful interference with goods in civil proceedings.

---

[54] The interest protected in the tort of trespass is possession. Although the plaintiff is not, in the current scenario, deprived of possession of the computer, the plaintiff is prevented from using that computer, either because the virus has caused it to stop operating, or because the plaintiff fears transmitting the virus to someone else.

152 Authorities differ as to whether intention is a necessary element of the tort of trespass to goods. The authors of *The Law of Torts in New Zealand* suggest that trespass should be regarded as a purely intentional tort, and that unintended acts should be actionable in negligence (Todd et al 1997 para 11.2.1). However, in *Wilson v New Brighton Panelbeaters* [1989] 1 NZLR 74, 77 Tipping J appeared to assume that unintended interference with goods is trespass provided there is evidence of damage.[55] Similarly, in *National Coal Board v JE Evans & Co Ltd* [1951] 2 KB 861 the English Court of Appeal held that the wrongful interference with the plaintiff's goods must at least be negligent for there to be any liability in trespass.[56]

153 On this basis, liability in trespass for wrongfully transmitting a computer virus does not necessarily require knowledge of the existence of the virus on the part of the defendant. It will be sufficient if the defendant *should* have known of the existence of the virus and failed to take adequate precautions to prevent its transmission. This raises the question of what constitutes an adequate standard of care against infection by or transmission of computer viruses; this issue is addressed in paras 172–176. However, unlike the tort of negligence, there is no need to prove that the damage suffered by the plaintiff was foreseeable by the defendant (Todd et al, para 11.2.4; *Mayfair Ltd v Pears* [1987] 1 NZLR 459; see also para 175 of this report).

The nature of the damage

154 Damage caused by a computer virus is not of a physical nature. The computer, or rather the storage device (such as a hard disc) within which data is recorded, is not rendered inoperative in any physical sense. Rather, it is prevented from operating properly. It

---

[55] It is not necessary for me in this case to discuss the more difficult questions of whether or not an unintentional interference with goods is actionable without proof of damage, and indeed whether damage or asportation is necessary to constitute the tort. . . . (77)

This in turn draws on the earlier case of *Everitt v Martin* [1953] NZLR 298.

[56] In this case, the defendant damaged a buried electricity cable belonging to the plaintiff. However, this interference was not tortious because the cable had been buried on the defendant's land without the defendant's knowledge or consent, and did not appear on any plan. The interference was therefore neither intentional nor negligent. Note also that it is not tortious for a defendant to interfere with goods if he or she is entitled to exercise a self-help remedy, such as removing goods which have been unlawfully placed on his or her land (Laws NZ, *Torts*, para 291).

is also possible that data stored on the computer may be lost (Gringras 1997 66–69). The loss caused to a business by virus infection may therefore include:

- the cost of restoring the computer(s) to an operational state;
- the value of any data lost;
- loss of profits for the time that business or production is incapacitated; and
- loss of reputation or goodwill.

155 The damages available in trespass include the cost of repairing the goods, loss of profits or use of the goods, and in appropriate cases, exemplary damages. Where there is a risk of the interference continuing or being repeated, injunctive relief may also be available (Laws NZ, *Tort*, paras 285–286).

156 There is a duty imposed on plaintiffs at common law to take reasonable steps to mitigate losses (Laws NZ, *Tort*, para 43). However, it should be noted that this duty only arises after the damage has been caused. Thus, the law (as well as commercial good sense) requires a business whose computers are infected with a virus to respond quickly. But there would be no penalty for failing to take steps before the damage occurred; for example, losses caused by failure to back up a computer on a regular basis would not constitute a failure to mitigate losses, because that failure occurred *before* the wrongful interference occurred.

157 Views have been expressed that a defence of contributory negligence may be available in response to an action based on trespass to goods; for example, in *Dairy Containers Ltd v NZI Bank Ltd* [1995] 2 NZLR 30, Thomas J came to that conclusion after analysing the Contributory Negligence Act 1947. This view is not firmly established and has been the subject of academic criticism (Todd et al 1997 para 21.1.4(a)). The law remains unsettled in this area. The Law Commission recommended in its recent report, *Apportionment of Civil Liability* (NZLC R47 1998), that the whole of the law regarding contribution in civil cases be reformed and if that reform is enacted it will be possible to raise contributory conduct by way of defence. Having regard to the views expressed in *Apportionment of Civil Liability* the Commission does not consider it necessary to embark upon a reconsideration of this issue in this context.

CONFIDENTIAL INFORMATION

158 Although the action for breach of confidence has its origins in equity rather than tort, we include it in this discussion because of the likelihood that confidential information will be stored elec-

tronically. The extent to which the law is able to protect businesses who store confidential information is therefore of importance.

159 Liability for breach of confidence typically (although not necessarily always) arises in equity when information which is confidential[57] is imparted in circumstances importing an obligation of confidence and that information is used by the confidant to the detriment of the confidor.[58] Remedies include injunctions to prohibit the disclosure of confidential information, orders for the delivery or destruction of the information, and damages.[59] It may not be necessary to prove that the defendant has caused harm to the plaintiff by unauthorised use of the confidential information[60] and the mere threat of improper use is a sufficient foundation for injunctive relief: *Ross Industries (New Zealand) Ltd v Talleys Fisheries* (unreported, HC, Auckland, 5/9/97, CP68/97), 3.

160 Electronic commerce has thrown some aspects of the law relating to breach of confidence into sharp focus. In particular the use of electronic communications technology raises essential questions about the availability of remedy when:

- confidential files are copied from a computer without the owner's consent; or
- electronic communications containing confidential information are intercepted by a third party.[61]

---

[57] The definition of confidential is broad and encompasses information as diverse as commercial trade secrets or client details, and personal secrets passed between spouses (see Laws NZ, *Intellectual Property: Confidential Information*, paras 22–43; and Meagher, Gummow and Lehane 1992 chapter 41).

[58] See Laws NZ, *Intellectual Property: Confidential Information*, para 17; *Saltman Engineering Co Ltd v Campbell Engineering Co Ltd* [1963] 3 All ER 413; *AB Consolidated Ltd v Europe Strength Food Co Pty Ltd* [1978] 2 NZLR 515, 520; and the recent decision of the Court of Appeal in *Maclean & Ors v Arklow Investments Ltd & Ors* (unreported, 16 July 1998, CA95/97).

[59] Laws NZ, *Intellectual Property: Confidential Information*, paras 144–146. See also *Aquaculture Corporation v New Zealand Green Mussel Co Ltd* [1990] 3 NZLR 299. Note, however, that because the remedy is equitable, all remedies are discretionary.

[60] Laws NZ, *Intellectual Property: Confidential Information*, para 17; see also *Attorney-General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109 (HL), 256, 282.

[61] Questions arising from the accidental communication of confidential information to the wrong person or wrongful use of confidential information by a person who originally acquired that information lawfully are not considered as such issues are not peculiar to the field of electronic commerce.

Unauthorised copying of confidential information

161 It is technically possible to obtain information from a computer in a way which does not give rise to liability in conversion or trespass to property. For example, where a computer is part of a network it may be possible for a hacker to penetrate security barriers and copy commercially sensitive or valuable files. In such a case, there may be no damage to the computer or the files on which to base an action for trespass to property. Similarly, because the files are copied rather than stolen, the owner is not deprived of possession, and may therefore be prevented from claiming damages for conversion. In any case, the remedy for conversion would in many cases be unsuitable because the defendant would be required to pay damages rather than destroy or deliver up the information. In the absence of any prior contractual or fiduciary relationship between the owner of the files and the hacker, and assuming the files are not protected by copyright, it is likely that breach of confidence will be the owner's only possible remedy.[62]

162 Whether a remedy for breach of confidence is in fact available is, however, somewhat uncertain. The traditional requirement that the information be imparted in circumstances giving rise to an obligation of confidentiality generally concerns a situation where A deliberately gives information to B in circumstances where A intends the information to be confidential and B is aware (or ought to be aware) of that fact. This differs from the scenario outlined above, because the information is not voluntarily imparted, but taken. In its 1981 report, *Breach of Confidence*, the Law Commission for England and Wales concluded at para 4.10:

> it is very doubtful to what extent, if at all, information becomes impressed with an obligation of confidence by reason solely of the reprehensible means by which it has been acquired, and irrespective of some special relationship between the person alleged to owe the obligation and the person to whom it is alleged to be owed.[63]

This position was described by the English Commission as a "glaring inadequacy" (para 5.5) and legislation was proposed which, among other things, would have imposed civil liability for improperly acquiring information by using or interfering with a computer or

---

[62] Nor would copying information constitute theft under current New Zealand law: Laws NZ, *Intellectual Property: Confidential Information*, para 182.

[63] See also the consultation paper of the Law Commission (England and Wales), *Legislating the Criminal Code: Misuse of Trade Secrets*, which discusses the case for criminal liability for certain misuses of confidential information.

data retrieval system without authority (cl 5(2)(a)(iii) of the Commission's yet to be enacted draft Breach of Confidence Bill).

163 Notwithstanding the view of the English Commission, this Commission believes that a person who obtains confidential information by reprehensible means is subject to a duty of confidence.[64] In *Franklin v Giddins* [1978] Qd R 72, 80, Dunn J stated that

> it would be extraordinary if a defendant, who acquired by eavesdropping or other improper covert means the secrets of the plaintiff because he would not have been able to get them by consensual arrangement, could defend proceedings by the plaintiff on the ground that no obligation of confidence could arise without communication of the information by the defendant.[65]

164 We believe this to be a correct statement of the law.[66] We note that in *Ross Industries (New Zealand) Ltd v Talleys Fisheries Ltd*, the proposition that a duty of confidence can only arise in the context of relationship of trust or confidence between the parties was specifically rejected by the court. The Commission is of the opinion that an adequate remedy is available when confidential information is stolen from a computer by a hacker. However, we invite submissions as to whether a statutory remedy of breach of confidence should be enacted. In doing so we express a strong provisional inclination to the view that a statutory remedy could not readily be justified for the electronic environment alone. The nature of the electronic environment simply throws the problems into sharper focus.

---

[64] Note that the duty is not limited to the party who obtains the information; it can also extend to innocent third parties who subsequently obtain a copy: *Ross Industries (New Zealand) Ltd v Talleys Fisheries*.

[65] The fact situation in *Franklin* is directly analogous. The action concerned early fruiting nectarine hybrids which could only be raised by grafting a cutting (budstock) on to rootstock, which were bred by the plaintiff. The defendant stole cuttings from the plaintiff, grafted them, and made further cuttings from the resulting trees until he had an orchard. Although the possibility remained of bringing proceedings for conversion of the cuttings, the plaintiff preferred breach of confidence because the effective remedy in conversion would be a forced sale of the trees to the defendant. The plaintiff had no intention of letting others benefit from his work, a fact of which the defendant was well aware; rather, he wanted the defendant's trees destroyed. Although there was no prior relationship of confidence between the parties, the court allowed the plaintiff to succeed.

[66] See also Meagher, Gummow and Lehane 1992 para 4109; Laws NZ, *Intellectual Property: Confidential Information*, para 115, and the cases cited there. See also the dicta of Lord Goff of Chievelely in *Attorney-General v Guardian Newspapers Ltd* [1988] 3 All ER 545, 658–659; and Denning 1982 264–268.

Unauthorised interception of communications

165 In *Malone v Metropolitan Police Commissioner* [1979] Ch 344, Megarry V-C held that no duty of confidence attaches to information acquired by interception of a telephone conversation:

> It seems to me that a person who utters confidential information must accept the risk of any unknown overhearing that is inherent in the circumstances of communication. . . .
>
> When this is applied to telephone conversations, it appears to me that the speaker is taking such risks of being overheard as are inherent in the system. . . . No doubt a person who uses a telephone to give confidential information to another may do so in such a way as to impose an obligation of confidence on that other; but I do not see how it could be said that any such obligation is imposed on those who overhear the conversation, whether by means of tapping or otherwise. (376)

Megarry V-C was careful to limit the above statement to the facts of the particular case – tapping conducted by the Post Office on Post Office premises at the request of police who in turn were acting pursuant to a warrant (383–384). But it apparently remains open to argue that no obligation of confidence attaches to the person who intercepts electronic communications, because parties who use electronic communication are deemed to have accepted the risk of messages being intercepted.

166 Although the Commission acknowledges the law is uncertain, we consider that a person who without authority intercepts a message containing confidential information would be subject to a duty of confidence. In reaching this conclusion, we note that while *Malone v Metropolitan Police Commissioner* has never been overruled, and has not been held inapplicable in New Zealand, it seems to have been limited to its facts in England. In *Francome v Mirror Group Newspapers Ltd* [1984] 1 WLR 892, 895, Sir John Donaldson MR referred to the decision as "somewhat surprising", and Meagher, Gummow and Lehane regard it as being wrongly decided (1992

---

[67] See also Fox LJ in *Francome v Mirror Group Newspapers Ltd* [1984] 1 WLR 892, 899–900, and the dicta of Swinfen Eady LJ in *Ashburton v Pape* [1913] 2 Ch 469, 475. *Francome* concerned information obtained by means of an illegal wire tap which the defendant, a newspaper, subsequently obtained and attempted to publish. The Court of Appeal ordered an interlocutory injunction prohibiting publication to preserve the position of the parties until trial, but did not consider that *Malone* compelled the court to deny the existence of a duty of confidence (Meagher, Gummow and Lehane 1992 para 4109).

para 4109).[67] However, until such time as a court holds that the interception of electronic communications imposes a duty of confidence on the person who obtains the confidential information, uncertainty is likely to continue. Once again, we invite comment on whether statutory reform is necessary to remove this uncertainty.

Is a statutory remedy of breach of confidence necessary to impose civil liability for unauthorised copying or interception of confidential information?

NEGLIGENCE

167 Liability for the tort of negligence arises when a duty of care owed to another is breached and loss is caused to that person as a result of the breach. The topic is vast, and the categories of negligence are not closed. It is therefore likely that new commercial and communications practices will in time lead to developments in the law of negligence. For the purposes of this paper, however, we focus on two discrete issues which are of particular relevance to electronic commerce: transmission of viruses and liability for advice.

Duty of care

168 In order to establish liability for a negligent act or omission it is first necessary to establish that the defendant owes a duty of care to the plaintiff. This may be accomplished because the case falls within a recognised duty of care, such as liability for a false statement (eg, an action for negligent misrepresentation: see *Hedley Byrne & Co Ltd v Heller & Partners Ltd* [1963] AC 465). If, however, the case falls outside the scope of established duties, it is necessary to consider the principles set out by the House of Lords in *Anns v London Borough of Merton* [1978] AC 728:[68]

> First one has to ask whether, as between the alleged wrongdoer and

---

[68] This approach to novel cases has been adopted by the Court of Appeal: see *South Pacific Manufacturing Co Ltd v New Zealand Security Consultants Ltd* [1992] 2 NZLR 282, 294; *Connell v Odlum* [1993] 2 NZLR 257, 265; and *Fleming v Securities Commission* [1995] 2 NZLR 514, 526–527. Although the courts in the United Kingdom have moved from the position adopted in *Anns v London Borough of Merton*, it has been confirmed that the law of negligence is one area in which the common law of New Zealand is diverging from that of England: *Hamlin v Invercargill City Council* [1996] 1 NZLR 513. Accordingly, the above statement remains an accurate statement of the law in New Zealand.

> the person who has suffered damage there is a sufficient relationship of proximity or neighbourhood such that, in the reasonable contemplation of the former, carelessness on his part may be likely to cause damage to the latter, in which case a prima facie duty of care arises. Secondly, if the first question is answered affirmatively, it is necessary to consider whether there are any considerations which ought to negative, or to reduce or limit the scope of the duty or the class of person to whom it is owed or the damages to which a breach of it may give rise. (751)

169 In the context of electronic commerce, issues of proximity or neighbourhood are especially problematic. Who is one's "neighbour" in an electronic world? It is not unreasonable to regard a computer user as having a relationship of proximity with any other computer user with whom he or she is in contact, whether directly or indirectly. Thus, such a relationship would exist wherever information is transferred from one computer to another, either by means of a network or by the physical transfer of information through memory devices such as floppy discs or compact discs. In the case of an internet website, it would be reasonable to extend the relationship to anyone visiting the site. Indeed, it is at least possible to say that any computer network user should realise that negligence on his or her part may ultimately cause damage to any other user of the network, if a virus is transmitted. Thus, the inquiry regarding the nature of a duty of care on the internet is not likely to be whether such a duty could exist, but rather, the number of people to whom the duty is owed.

170 Indeed, Gripman has suggested in "The Doors are Locked but the Thieves and Vandals are Still Getting In" that a duty of care in negligence should be imposed on a business user of a computer system

> to prevent hacker intrusions that can severely damage the corporation itself or other internet-connected third party corporations damaged resulting from the original hacker intrusion. (1997 172)

The types of "hacker intrusion" to which Gripman refers are summarised as:

- infection of a computer network with a virus, and

---

[69] See also *Revlon Inc v Logisticon Inc* (unreported, Superior Court of California, Santa Clara County No 705933, complaint filed 22 October 1990). Gripman also refers to *United States v Morris* 928 F 2d 504, 505–506 (Second Circuit, 1991) which involved damage caused by a virus ranging between $96 million to $186 million based upon labour costs to eradicate the virus and monitor recovery of the computer system (171); in that regard see also Lyman, *Civil Remedies for the Victims of Computer Viruses* 21 Sw ULRev 1169, 1172 (1992).

- intentionally shutting down a computer system so that a company cannot distribute its products (Gripman 1997 170; also Robbins 1993 20).[69]

We return to deal with the steps that can be taken to protect a computer system when discussing the standard of care in paras 172–176.

171 The liability of an internet service provider (ISP) in negligence is problematic. However, unless the ISP can be regarded, properly, as an agent of a user or as having failed to take adequate steps to ensure that users of its services do not infect other users with viruses it is unlikely that an ISP would be liable in tort.

Standard of care

172 Where a duty of care exists, there is a legal obligation to exercise a reasonable standard of care:

> [S]omething which a reasonable man, guided upon those considerations which ordinarily regulate the conduct of human affairs, would do; or doing something which a prudent and reasonable man would not do. (*Blyth v Birmingham Waterworks Co* (1856) Ex Ch 781, 784)

Thus, if computer users owe a duty of care to others connected to the same network not to transmit viruses, the question becomes, what is a reasonable standard of care? Liability in negligence does not accrue if a defendant who causes the damage has nevertheless exercised a reasonable standard of care in his or her dealings with a plaintiff.

173 In assessing what is a reasonable standard of care, courts may take into account current industry practice and the nature of the particular virus.[70] The extent of the risk may be balanced against the cost and difficulty of taking precautions against that risk. Thus, the reasonableness of any particular set of precautions depends on the nature of the risk. The standard of care may also be elevated if the user claims to be an expert; in such a case, the appropriate

---

[70] This does not imply that a court must necessarily find that industry practice is sufficient to meet the legal standard of care where conformity with best practice guides does not constitute incontrovertible proof that the user has exercised a reasonable standard of care. Such evidence will be taken into account by a court in determining whether the allegation of negligence has been made out: *Bolam v Friern Hospital Management Committee* [1957] 1WLR 582; Laws NZ, *Negligence*, para 5.

standard would be that expected of a reasonable *expert*, in the field in which the user claims to be an expert. It follows from this that a company which regularly conducts business transactions via computer networks, or the operator of a popular website, may reasonably be expected to employ a higher level of precautions than a casual browser.

174 In general, the risk of transmitting a virus is great if the virus is one which affects commonly used computer software. Conversely, the cost and difficulty of installing software to guard against commonly occurring viruses is not great. However, it should be noted that the duty to take adequate precautions is not fixed in time. Rather, it is, "an obligation which keeps pace with the times. As the danger increases, so must . . . precautions increase": *Lloyds Bank v Railway Executive* [1952] 1 All ER 1248, 1253. Accordingly, merely installing virus protection software may not be an adequate precaution if that software is not regularly updated.

175 Determination of an appropriate standard of care is linked to the basic purposes of the law of tort. In a computer context Gripman has summarised these as follows:

- to deter wrongful conduct;
- to encourage socially responsible behaviour;
- to restore injured parties to their original condition by compensating them for their injuries (Gripman 1997 176).

There are technical means by which computer systems can be made more secure: examples are firewalls, and encryption technology.[71] It is also possible to acquire anti-viral programs. By acquiring such

---

[71] Gringras defines a "firewall" as:

> hardware, but more usually software, designed to protect network systems from damage by outsiders, while maintaining connectivity. The firewall sits between a local network and the big, wide world (usually the internet). To protect the local network from evil-intentioned intruders, the firewall may admit only designated users, or allow only designated commands to be issued from outside. Balancing flexibility with security is, needless to say, a perennial headache in designing firewalls. (Gringras 1997 382).

Encryption is the mathematical process used to disguise text or data. It takes two forms: those forms are public key encryption and private key encryption (Gringras 381). For further discussion of public and private key encryption see chapter 7.

[72] Gripman provides a useful analysis, in technical terms, of the steps that can be taken to minimise security problems in this context (1997 182–195); that is followed by a specific case study (191–195).

programmes and educating staff as to the problems that can arise through unauthorised entry to a computer system the possibility of breaching any standard of care may be minimised. It would be wise for those engaged in electronic commerce to take expert advice on protection measures that are open to them to minimise the prospect of being sued in tort.[72]

176 Historically, the law has imposed lower standards of care when a defendant is a minor (see, for example, *Spiers v Gordon* [1966] NZLR 897, and *Mullin v Richards* [1998] 1 WLR 1304). However tortious acts on the internet may be carried into effect by children of any age without knowledge of that from other persons operating within the internet at any particular time. Unless a child was too young or immature to form the requisite intent (for an intentional tort) it is likely that liability would exist. A separate duty (actionable at the suit of the injured person) may also arise against the minor's parents for failing to supervise the child's activities properly (Laws NZ, *Torts*, para 27).

Damage

177 A debate has raged for some time as to whether, in an action for negligence, the recovery of "pure" economic loss is possible. In New Zealand the courts have held that the distinctions drawn by the House of Lords in *Murphy v Brentwood District Council* [1991] 1 AC 398 (HL) do not apply in New Zealand. This view has subsequently been upheld by the Privy Council in a building case which held that the New Zealand courts were entitled to follow their own path in this regard: *Invercargill City Council v Hamlin* [1994] 3 NZLR 513 (CA); appeal dismissed [1996] 1 NZLR 513 (PC).

178 The real issue in the context of electronic commerce is whether there are any policy considerations that would justify limiting the scope of a duty of care based on the formulation in *Anns v London Borough of Merton* [1978] AC 728. Some of the issues which need to be addressed in that regard are:

- The seriousness of harm that will be caused and the seriousness of the foreseeable consequences: *South Pacific Manufacturing Co Ltd v New Zealand Security Consultants Limited* [1992] 2 NZLR 282 (CA) 295.

- The "floodgates" argument – the courts will not wish to impose a liability that is potentially indeterminate:

  > A simple requirement that harm be foreseeable may provide no adequate control over the potential ambit of liability, so more

> restrictive tests may need to be applied. Thus the courts may require specific knowledge or foresight on the part of the defendant of exactly who would suffer harm and how it would come about and what form it would take. (Todd et al 1997 para 4.3.3)

- Reasonable alternative opportunities for self protection – a number of recent decisions support the proposition that it is relevant to take into account the extent to which the plaintiff could have used adequate alternative opportunities for self protection (Todd et all para 4.3.5; see also *South Pacific Manufacturing Co Ltd v New Zealand Security Consultants Limited* and *Henderson v Merrett Syndicates Limited* [1995] 2 AC 145 (HL)). Into this category come concerns that:
  - the court should not allow a plaintiff greater recovery in tort than he or she was prepared to pay for in contract;
  - whether the plaintiff had or could have some alternative right of recourse against the defendant (eg, where a plaintiff could have bargained for protection in contract); and
  - whether insurance is available for the type of loss involved; and if not, why not?

179 Sometimes exemplary damages are sought. Exemplary damages are damages which are designed to punish conduct rather than to provide compensation. They are usually awarded for intentional actions. The Court of Appeal has made it clear that exemplary damages are available in negligence in only the most exceptional cases: *Ellison v L* [1998] 1 NZLR 416 (CA), 419.

Causation

180 In negligence proceedings, the plaintiff is required to prove that there is a causal connection between the defendant's negligent act or omission and the plaintiff's damage. This is not merely a question of determining that the defendant's act or omission is a factual cause of the plaintiff's loss; the plaintiff must also prove that the defendant's negligence and the plaintiff's damage are sufficiently closely connected (see generaly Todd et al 1997 chapter 20). In other words, liability is limited on policy grounds when the harm is considered to be too remote from the negligence: *Overseas Tankship (UK) Ltd v Morts Dock and Engineering Co Ltd, The Wagon Mound (No 1)* [1961] AC 388.

181 In the context of computer networks, the need to prove causation may be of particular importance in cases where a plaintiff's computer or website has been infected several times by the same virus. Multiple infections by the same virus will not usually cause more damage than a single infection; it would therefore be a complete

defence to prove that the plaintiff's computer was already infected when the defendant transmitted the virus.

182 The issue of remoteness of damage may arise when the plaintiff's computer or website has not been infected by direct contact with the defendant. Although there would be little difficulty in establishing that the defendant's negligent dissemination of a virus is a *factual* cause of the plaintiff's loss, it may not be a *legal* cause if the plaintiff is too remote from the defendant (Gringras 1997 73–76). Several factors may be relevant to this issue:

- the number of intermediaries between the defendant and the plaintiff; and
- whether any of those intermediaries acted in such a way as to break the chain of causation.

Liability for advice: negligent misstatement

183 Liability in tort for loss caused by false or negligent advice is not an issue which raises particular problems for those engaging in electronic commerce. However, because advice is a product which can be delivered electronically, it is an area of commerce which can realistically be expected to reap the maximum gain from electronic communications.

184 The duty of care (in the context of negligent advice) has been summarised by Lord Oliver in *Caparo Industries plc v Dickman* [1990] 2 AC 605 (HL) thus:

> [T]he necessary relationship between the maker of a statement or giver of advice ('the adviser') and the recipient who acts in reliance upon it ('the advisee') may typically be held to exist where
> (1) the advice is required for a purpose, whether particularly specified or generally described, which is made known, either actually or inferentially, to the adviser at the time when the advice is given;
> (2) the adviser knows, either actually or inferentially, that his advice will be communicated to the advisee, either specifically or as a member of an ascertainable class, in order that it should be used by the advisee for that purpose;
> (3) it is known, either actually or inferentially, that the advice so communicated is likely to be acted upon by the advisee for that purpose without independent inquiry; and
> (4) it is so acted upon by the advisee to his detriment. (638)

185 The third requirement that the advisee be known to the adviser, either specifically or as a member of an ascertainable class, would preclude liability where advice is published on a website and relied on by a browser. But the same may not be true if an advisee forwards the advice to a third party who *does* meet the test.

DEFAMATION

186 The tort of defamation protects the reputation of an individual against false or unjustified allegations. It is established when the plaintiff proves that

- a defamatory statement was made; and
- that statement was about (identified) the plaintiff; and
- the defendant published the statement (see generally Todd et al 1997 chapter 16).

187 There is little doubt that electronic transmission of a defamatory statement which identifies the plaintiff constitutes publication for which the publisher will be liable: *Rindos v Hardwick* (unreported, 31/3/1994, SC WA Ipp J, 164/1994); see 6(1) *Laws of Australia* paras 18–19. Publication merely requires that the defamatory statement be made to a person other than the plaintiff. The statement may be written or spoken as New Zealand law, under the Defamation Act 1992, does not distinguish between different forms of publication. Thus, forwarding email containing a defamatory statement to a person other than the plaintiff, or downloading such a statement from the internet, could give rise to liability in defamation, regardless of the identity of the original maker of the statement. Indeed, a recent case has held that merely publishing the URL[73] address of a website which in turn contains defamatory statements *may* constitute republication of that article: *International Telephone Link Pty Ltd v IDG Communications Ltd* (unreported, HC, Auckland, 20 February 1998, CP344/97). 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.

188 Two American cases have considered the liability of network providers for defamatory statements. In *Cubby, Inc v CompuServe Inc* 776 F Supp 135 (SDNY 1991), CompuServe, an ISP, was held not liable for republishing defamatory statements contained in an online newsletter which was written by a separate company. This decision turned on the fact that CompuServe did not exercise editorial control over content in the newsletter; nor did it have

---

[73] The acronym URL stands for uniform resource locator and refers to the standard for specifying an object on the internet, such as a world wide web page or a file on a file transfer protocol (FTP) for example. A URL for the world wide web will have the prefix "http://" denoting that the page uses hyper-text transfer protocol (see Gringras 1997, 387).

knowledge of content:

> CompuServe has no more editorial control over such a publication than does a public library, bookstore or news-stand, and it would be no more feasible for CompuServe to examine every publication it carries for potential defamatory statements than it would be for any other distributor to do so. (140)

189 However, in *Stratton Oakmont Inc v Prodigy Services Inc* NYS 2d Index No 31063/94, [1995] WL 323710, Prodigy (another ISP) was held liable in defamation because it exercised a degree of editorial control over the content of material published on a bulletin board. Prodigy advertised itself as a family-oriented computer network, employed software to screen messages for offensive language before they were published on the bulletin board, and required subscribers to adhere to content guidelines. It also appointed "Board Leaders" to enforce those guidelines, and provided them with the ability to delete messages which contravened the guidelines. This control did not necessarily mean that Prodigy, or any of its agents, had actual knowledge of the defamatory statement, leading at least one commentator to observe that the practical effect is to encourage a "hands off" approach on the part of ISPs (Carey 1997 1634).

190 Defamation law in New Zealand is governed by the Defamation Act 1992. Section 21 of that Act provides that a person who publishes defamatory material as a "processor or distributor"[74] has a defence of innocent dissemination if

> that person alleges and proves
> (a) That that person did not know that the matter contained the material that is alleged to be defamatory; and
> (b) That that person did not know that the matter was of a character likely to contain material of a defamatory nature; and
> (c) That that person's lack of knowledge was not due to any negligence on that person's part.

Whether a New Zealand ISP could be liable on the same fact situations as arose in *Cubby* and *Stratton Oakmont* would therefore depend on proving lack of knowledge without negligence. The standard of care in such circumstances would need to take into account the relevant standard practice of the industry together with any public policy issues such as whether or not a duty should be placed on ISPs to censor the material placed on their network

---

[74] The definitions of "processor" and "distributor" in s 2(1) of the Defamation Act 1992 are probably sufficiently broad to include computer network service providers (see Todd et al 1997 882).

by their clients, and if so, in what circumstances.

CONCLUSION

191 We seek submissions as to whether legislation is necessary to limit the boundaries of liability in tort having regard to the problems in defining one's neighbourhood in an electronic environment. Any legislation to limit the boundaries of the law of torts would have to be based firmly on the floodgates principle: that it is necessary to prevent persons trading or operating on the internet from being exposed to "liability in an indeterminate amount for an indeterminate time to an indeterminate class": *Ultra Mares Corporation v Touche* NY Rep 170, 174 (1931).

192 Should submissions be made which can justify the need for legislation to curb potential liability in tort, we will address those issues in our second report. Our provisional view is that legislation would not be feasible because of the difficulty in articulating any restrictions in a sensible and workable manner.

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?

Select bibliography

REPORT

Attorney-General's Department of Australia, *Review of Commonwealth Criminal Law: Interim Report, Computer Crime* (November 1988)

Crimes Consultative Committee, *Crimes Bill 1989, Report of Crimes Consultative Committee* (April 1991)

Dishonestly Procuring Valuable Benefits (NZLC R51, December 1998)

Electronic Commerce Part One: A guide for the Legal and Business Community (NZLC R50, October 1998)

Law Commission of England and Wales, *Criminal Law: Computer Misuse* (Law Com. No. 186, 1989)

Privacy Commissioner, *Necessary and Desirable: Privacy Act 1993 Review* (November 1998)

Scottish Law Commission, *Report on Computer Misuse* (Scot Law Com, No 106 1987)

South African Law Commission, *Computer Related Crime* (Issue Paper 14, August 1998)

TEXTS

Gringras, *The Laws of the Internet* (Butterworths, London, 1997)

Robertson et al, *Adams on Criminal Law* (Brooker $ Friend Ltd, 1992)

Smith & Hogan, *Criminal Law* (17th ed. 1992)

ARTICLES AND PAPERS

Gripman, *The Doors are Locked but the Thieves and Vandals are still getting In: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem* (1997) 16 Journal of Computer and Information Law 167

Hon Maurice Williamson MP, *Wealth & Wellbeing in a Networked World*, (New Zealand Law Society Conference Paper, April 1999)

Moller, *Protective Measures Against Compromising Electromagnetic Radiation Emitted by Video Display Terminals*, Phrack Magazine, Vol 4, Issue 44

Wim Van Eck, *Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk*, Computers & Security 4 (1985) 269-286

INDEX