14. Cybercrime and Jurisdiction in New Zealand

Noel Cox*

14.1. Introduction

There are comparatively few specific legislative provisions in New Zealand relating to cybercrimes. The general approach has been to amend general criminal provisions where necessary to address specific problems presented by cybercrimes, but not to treat these as being inherently different to crimes committed through more traditional media.

Just as the legislative provisions do not generally treat cybercrimes as *sui generis*, so there is not a generic enforcement agency charged with the detection of cybercrime and the prosecution of cybercriminals. For similar reasons there are few specific provisions with respect to cybercrime jurisdiction. There also remains a reluctance to assert an extraterritorial jurisdiction over cybercrime *per se*, though there are aspects of this in recent legislation covering terrorist-related offences.

The New Zealand Police[1] (the sole uniformed police agency in the country), the Department of Internal Affairs[2] (which has, *inter alia*, general responsibility for the censorship and classification of books and films) and the New Zealand Customs Service[3] (which is responsible for the enforcement of importation controls) are the three principal agencies responsible for electronic crime detection and investigation in New Zealand. In very general terms, Internal Affairs focuses on action against Internet offending, the Police deal with physical offending and Customs with importation offences. Nearly a dozen other government agencies also deal with some aspects of computer-related offences. In most instances they enforce a combination of general criminal laws, and the comparatively few specific electronic or cyber-laws.

This chapter will explore some aspects of national cybercrime law in New Zealand, looking at both substantive law and the broader question of jurisdiction.

14.2. National Cybercrime Legislation

14.2.1. Brief History

Until 2002 there was, in New Zealand, comparatively little legislative response to the advent of cyberspace and even of computers in general. The general criminal provisions were utilised in those instances where offences occurred in cyberspace or were committed through the use of computers. While this approach is not always entirely adequate, this was initially satisfactory given the relatively small number of reported cybercrime. The real level of crime may however have been significantly higher, due to an ignorance that offences (such

* Noel Cox is Associate Professor of Law at Auckland University of Technology, New Zealand.

[1] Police Act 1958 (NZ).

[2] Films, Videos and Publications Classification Act 1993 (NZ).

[3] Customs and Excise Act 1996 (NZ).

as identity theft) were occurring, or a lack of appreciation that computer-based crimes were distinct from crimes committed through traditional means (if indeed they are), or quantitatively or qualitatively significant.

Article 2 of the 2001 Council of Europe's Convention on Cybercrime[4] required signatory governments to enact such provisions as may be necessary to establish as criminal offences under their domestic laws, when committed intentionally, the access to the whole or any part of a computer system without right. Although New Zealand was not a signatory to this Council of Europe initiative, the Budapest convention is the first international agreement on the control of cybercrime; it has so far been signed by 42 countries,[5] and its influence could not be ignored. The principal New Zealand response – which was also influenced by recent cases highlighting difficulties with the pre-existing law – was to amend parts of the Crimes Act 1961, the primary legislative enactment providing procedures and penalties for serious crimes.

14.2.2. Provisions on Various Cybercrimes

Hacking and Related Offences

Unauthorised access to computer systems, or 'hacking', is restricted by the Telecommunications Act 1987 and more recently by amendments to the Crimes Act 1961. It is an offence to listen, record or disclose private communications between two or more people without authority. 'Private communications' are however confined to oral communications.

The case of *R* v. *Williamson*[6] had highlighted the legislative and common-law deficiencies with respect to electronic theft which led to the 2003 amendments to the Crimes Act 1961. There is still no specific crime for identity-related fraud or theft. This particular type of offence is, however, covered by a number of provisions in the Crimes Act 1961.

The four new crimes, part of the Crimes Act since 2003, are concerned primarily with hacking. They include:

1. Accessing a computer system for a dishonest purpose;[7]
2. Damaging or interfering with a computer system;[8]
3. Making, selling, or distributing or possessing software for committing a crime;[9]
4. Accessing a computer system without authorisation.[10]

Accessing a computer system for a dishonest purpose (i.e., obtaining advantage or benefit or causing loss to another person) is subject to a maximum penalty of

---

[4] Council of Europe, Convention on Cybercrime (CETS 185) (November 23, 2001), http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[5] As per July 31, 2005. See Council of Europe, Convention on Cybercrime, Chart of Signatures and Ratifications, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=31/07/2005&CL=ENG.

[6] [1999] 1 NZLR 403.

[7] S. 249.

[8] S. 250.

[9] S. 251.

[10] S. 252.

seven years' imprisonment,[11] or a maximum of five years' imprisonment for accessing with this intent, even if the attempt is not successful.[12]

Damaging or interfering with a computer system is subject to a maximum of ten years' imprisonment where damage or interference is likely to be life threatening, and to a maximum of seven years otherwise. The statute provides that damaging or interfering is defined as where the offender:

> damages, deletes adds to, modifies, or otherwise interferes with or impairs any data or software in any computer system; or causes any of the above, or causes any computer system to fail or deny service to authorised users.

Making, selling, or distributing or possessing software for committing crime has a maximum penalty of two years' imprisonment. Making, selling or distributing applies to software which would enable another person to access a computer system without authorisation with the sole or principal purpose to commit a crime, or if they hold it out as being useful to commit a crime (regardless of any other legitimate use). Possession of software is only a crime when the software would enable the user to access a computer system without authorisation, and the user intends to use that software to commit a crime.

Accessing a computer system without authorisation has a maximum penalty of two years' imprisonment, and applies to anyone who intentionally accesses a computer system, directly or indirectly, knowing that they are not authorised to access that computer system, or when they are reckless as to whether or not they are authorised. This crime does not apply to people who are authorised to access a computer system if they access that system for a purpose other than the one for which that person was given access. Law-enforcement agencies, the Security Intelligence Service (SIS), and the Government Communications Security Bureau (GCSB) are also exempt from this section when they possess appropriate warrants.

The existing ban on listening devices has been extended to include any interception device. The definition of an interception device is 'any electronic, mechanical, electromagnetic, optical or electro-optical instrument, apparatus, equipment, or other device that is used or is capable of being used to intercept a private communication.'[13] Offenders are now liable to imprisonment for a term not exceeding two years if they intentionally intercept any private communication by means of an interception device. They are also liable for up to two years' imprisonment for disclosure of the communication, or even disclosing the existence of it.

Computer Fraud and Identity Theft

The case of *R* v. *Misic*[14] illustrates the general legal position in New Zealand with respect to computer fraud. Misic downloaded onto his computer from the Internet a programme which enabled him to arrange to make telephone calls overseas without being charged for them. He then operated a system whereby

---

[11] S. 249(1).
[12] S. 249(2).
[13] Crimes Act 1961 (NZ), s. 216A(1), definition of 'interception device'. Exceptions from this definition are made for hearing aids and other devices exempted by the Governor-General. See also *R* v. *Stephens* [1997] 3 NZLR 716; (1997) 15 CRNZ 308 (CA), discussing the meaning of 'intercept' and 'monitor' in s. 216A.
[14] [2001] 3 NZLR 1 (CA).

he and friends of his made a large number of overseas calls without paying a fee. He was charged under section 229A of the Crimes Act 1961 with obtaining documents with intent to defraud and with using documents with intent to defraud, namely the computer programme and the computer disk onto which the programme was loaded. After conviction, the accused appealed on the ground that neither the programme nor the disk was a 'document' for the purposes of section 229A, to which no statutory definition of 'document' applied.

The court held that a computer programme and the computer disk were documents for the purposes of section 229A. A document was a thing which provided evidence or information or served as a record.[15] The fact that the offence was committed through the use of a computer and the Internet did not present significant legal difficulties for the court, which simply applied the pre-existing common law to the new circumstances.

Another of the leading cases illustrating the legal situation prior to the enactment of the 2003 amendments to the Crimes Act 1961 is *R* v. *Garrett (No 2)*.[16] Andrew Garrett was prosecuted for identity-theft crimes, through the use of a Trojan horse programme, Back Orifice, attached to a game called Potato. He was charged under section 298 Crimes Act 1961 and was subject to a potential maximum five years' imprisonment. Garrett distributed the game by email, knowing that when the recipient opened the email it would infect his or her computer with the Back Orifice programme. During the trial there were legal arguments over whether sending a programme like this could amount to willful damage of the software of the recipient's computer.

The court held, on the basis of authority in *Misic*, that a computer programme is a document. The login information and passwords were obtained through the computer programme that was stored on the hard drive of Garrett's computer and therefore constituted a document. Garrett then took the document and reproduced it on his own computer. There was also evidence that the purpose for obtaining the login and password was to obtain a privilege, benefit or advantage, and thus constituted illegally using a document for pecuniary advantage. This again was an example of courts applying essentially pre-computer provisions in a new environment.

Identity-theft provisions of the Crimes Act 1961 may be summarised including the following – accessing a computer system for a dishonest purpose (s. 249), creating and distributing software for a criminal purpose (s. 251), hacking (s. 252), fraud (s. 229A) and identity theft (s. 298). These are generally pre-computer provisions, or derived from pre-computer provisions.

Objectionable Material

Besides provisions with respect to hacking and fraud, there are also specific provisions relating to objectionable material. The Films, Videos and Publications Classifications Act 1993 defines what material is classified as 'age-restricted' and what material is 'objectionable.' 'Possess' is also defined in section 131 of the Act. This particular section has presented some difficulties with respect to Internet pornography which is viewed on a computer but not

---

[15] See paras. 31 and 33 of the judgement. *Snow* v. *Hawthorn* [1969] NZLR 776 was approved, and *Grant* v. *Southwestern and County Properties Ltd* [1975] Ch 185; [1974] 2 All ER 465 was adopted.

[16] [2001] DCR 912 (Judge Harvey).

specifically saved to the hard drive or a disk. There have also been some difficulties with the definition of 'objectionable.'

The offences under the Films, Videos, and Publications Classification Act 1993 which are most regularly committed are those relating to possession. Not only will offenders be liable for publishing objectionable material, but they will also be liable for possessing it within their electronic systems, in particular, within the hard drive of a computer stored on files, or sent and received as e-mail.[17]

Moreover, the Act does not apply to broadcasts on media such as television, radio or the Internet because the definition of publication does not include broadcasts, and in particular, live broadcasts cannot be covered by the Act since no recording of them exists until after transmission.[18]

Internet Gambling

Internet gambling is also regulated, though only incidentally to the regulation of traditional gambling. The Department of Internal Affairs licenses gambling under the Gaming and Lotteries Act 1977. Under current law is it theoretically possible for an Internet gambling site to be granted a licence, though none has ever been granted. However, proposed changes to the law would prohibit Internet gambling sites in New Zealand, other than the official betting agency (the 'TAB') established under the Racing Act 2003.

There are currently no legal Internet gambling sites based on New Zealand, other than the TAB. There are special rules for the TAB itself that allow it to take Internet bets, but 'cyber-casinos' *per se* are prohibited.

14.2.3. Investigation Powers

In 1979, provisions were enacted criminalising the unauthorised use of interception devices to intercept private communications.[19] However these provisions do not apply where the person intercepting the communication is a party to it, or does so pursuant to a statutory authority to intercept the communication.[20] It is also lawful for the Police to use an interception device to intercept a private communication where there is an emergency and there are reasonable grounds for believing that the person making the communication is threatening the life of or threatening serious harm to another.[21]

---

[17] In *Goodin* v. *Department of Internal Affairs* [2003] NZAR 434, the Court found that the definition of 'publication' in the Films, Videos, and Publications Classification Act 1993 (NZ) encompassed computer disks (including hard drives), folders and files stored on computer disks, and images stored in such folders or files.

[18] Films, Videos, and Publications Classification Act 1993 (NZ), s. 2, definition of 'publication'. 'Exhibit' in relation to a sound recording, means to play that sound recording: s. 2, definition of 'exhibit'. Ordinary criminal provisions might cover live broadcasts, where, for example, indecent or obscene language was used, although these provisions would apply to the speaker and not to the broadcaster.

[19] Crimes Act 1961 (NZ), s. 216B, inserted by s. 2 of the Crimes Amendment Act 1979 (NZ).

[20] Crimes Act 1961 (NZ), s. 216B(2), as amended by the Crimes Amendment Act (No 2) 1997 (NZ), s. 4. The Acts authorising interception are the Crimes Act 1961 (NZ), Part XIA (ss. 312A-312Q), Telecommunications (Residual Provisions) Act 1987 (NZ), Part I (ss. 2-20) or the Telecommunications Act 2001 (NZ), New Zealand Security Intelligence Service Act 1969 (NZ), Government Communications Security Bureau Act 2003 (NZ), Misuse of Drugs Amendment Act 1978 (NZ), and the International Terrorism (Emergency Powers) Act 1987 (NZ).

[21] Crimes Act 1961 (NZ), s. 216B(3)(a) and (b). The use of the device must be authorised by a commissioned officer.

The interception of communications is governed by the Government Communications Security Bureau Act 2003. This allows the interception of communications pursuant to an interception warrant,[22] but not of domestic communications.[23] The New Zealand Security Intelligence Service Act 1969 provides for the issuance of domestic interception warrants.[24]

The interception of private communications by an interception device operated by a person engaged in providing an Internet or other communication service to the public is permitted if the interception is carried out by an employee of the person providing that Internet or other communication service to the public in the course of that person's duties. It is lawful for the interception to be carried out if it is necessary for the purpose of maintaining the Internet or other communication service.[25]

Section 198 of the Summary Proceedings Act 1957[26] gives power to a police constable to require a person who owns or works a particular computer to provide assistance in obtaining information from the computer. This raises important questions with respect to the New Zealand Bill of Rights Act 1990. In particular the computer provision raises the prospect of individuals being compelled to assist a constable to obtain information from a computer, although in so doing they may be incriminating themselves. This could be in breach of sections 25(c) and (d) of the New Zealand Bill of Rights Act 1990, which are the right to be presumed innocent until proved guilty according to law, and the right of everyone charged with an offence not to be compelled to be a witness or to confess guilt.

Everyone also has the right to be secure against unreasonable search or seizure, whether of the person, property, correspondence, or otherwise.[27] A search or seizure authorised by a valid statutory enactment will not contravene the Bill of Rights unless it is carried out in an unreasonable manner,[28] or the statutory provision which permits it is exercised unreasonably.[29] The general power to search a personal computer or laptop is based on provisions of the Summary Proceedings Act 1957, and on specific provisions with respect to indecent publications.[30]

On written application, a District Court Judge, Justice, Community Magistrate, or Registrar (who is not also a constable) may issue a search warrant in the prescribed form if satisfied of certain matters.[31] He or she must be satisfied that reasonable grounds exist for believing that, in any building,

---

[22] S. 15.
[23] S. 14.
[24] S. 4.
[25] Crimes Act 1961 (NZ), s. 216B(5) as inserted by the Crimes Amendment Act 2003 (NZ), s. 10.
[26] As amended by s. 3 Summary Proceedings Amendment Act 2003 (NZ).
[27] New Zealand Bill of Rights Act 1990 (NZ), s. 21. The specific statutory reference to 'person, property, or correspondence or otherwise' suggests a wider definition of search and seizure than was the situation at common law. This interpretation has been confirmed by decisions dealing with s. 21 of the New Zealand Bill of Rights Act 1990 (NZ). It has been held that a 'search' is an examination of a person and a 'seizure' is a taking of what is discovered: *R* v. *Jefferies* [1994] 1 NZLR 290, 300; (1993) 10 CRNZ 202, 214 per Richardson J (CA).
[28] *R* v. *Davis* (1993) 10 CRNZ 327 (CA), and see *R* v. *A* [1994] 1 NZLR 429 (CA).
[29] *R* v. *Laugalis* (1993) 10 CRNZ 350 (CA) and *R* v. *Ririnui* [1994] 2 NZLR 439; (1993) 11 CRNZ 435 (CA).
[30] Films, Videos and Publications Classifications Act 1993 (NZ).
[31] Summary Proceedings Act 1957 (NZ), s. 198(1), as amended by the Summary Proceedings Amendment Act (No 2) 1998 (NZ), s. 50(a). The prescribed form is Form 50 in the First Schedule to the Summary Proceedings Regulations 1958 (RPT 1980/84) (NZ). See *R* v. *Sanders* [1994] 3 NZLR 450 (CA).

aircraft, ship, carriage, vehicle, box, receptacle, premises, or place, there is any of the following. First, any thing upon or in respect of which any offence punishable by imprisonment has been or is suspected of having been committed. Second, any thing which there is reasonable ground to believe will be evidence as to the commission of any such offence. Third, any thing which there is reasonable ground to believe is intended to be used for the purposes of committing any such offence.[32] This procedure may be used to authorise the search of a computer.

In addition, but in a more limited context, the Films, Videos and Publications Classifications Act 1993 confers a power upon inspectors of publications to search for indecent material which are on public display,[33] and for the issue of search warrants to search for and seize indecent publications elsewhere.[34] While the former might conceivably be able to discover some computer-based pornography, for instance, the latter power is more likely to be relevant to searching computers for illicit material of one sort or another.

It is not clear whether enforcement agencies have a power to conduct remote searches of computer systems. The parliamentary Select Committee which considered the Crimes Amendment Bill (No 6), which was enacted as the Crimes Amendment Act 2003, declined to exclude this power as had been requested by the Privacy Commissioner,[35] saying the purpose of the Bill was to preserve existing powers, and they did not feel it gave law-enforcement agencies additional powers. But the Bill, and the (then) un-amended Crimes Act 1961, did not expressly authorise the remote searching of computers.

Another controversial issue was whether the SIS and GCSB would be able to use keyword searching and filtering, which is regarded as more invasive than other forms of monitoring due to its indiscriminate nature. The Select Committee examining the 2003 Bill also considered that the requirements for explicit warrants were adequate to deal with this, though others disagreed.

14.3. Jurisdiction for Cybercrimes

14.3.1. Provisions in Law

The standard provisions with respect to cybercrime jurisdiction are those contained in section 7 of the Crimes Act 1961 (as currently enacted):

> 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.[36]

This confines general jurisdiction to events in New Zealand, though the perpetrators need not have been in New Zealand. Jurisdiction is wider with respect to certain specific offences:

---

[32] Summary Proceedings Act 1957 (NZ), s. 198(1).
[33] Films, Videos and Publications Classifications Act 1993 (NZ), s. 106.
[34] Films, Videos and Publications Classifications Act 1993 (NZ), s. 109.
[35] A statutory officer appointed under the Privacy Act 1993 (NZ).
[36] S. 7.

> Even if the acts or omissions alleged to constitute the offence occurred wholly outside New Zealand, proceedings may be brought for any offence against this Act committed in the course of carrying out a terrorist act (as defined in section 5(1) of the Terrorism Suppression Act 2002) or an offence against [several specific sections][37] —
>
> (a) if the person to be charged —
>
> (i) is a New Zealand citizen; or
> (ii) is ordinarily resident in New Zealand; or
> (iii) has been found in New Zealand and has not been extradited; or
> (iv) is a body corporate, or a corporation sole, incorporated under the law of New Zealand; or
>
> (b) if any of the acts or omissions is alleged to have occurred [on board a New Zealand-related ship or aircraft]; or
>
> (c) if a person in respect of whom the offence is alleged to have been committed
>
> (i) is a New Zealand citizen; or
> (ii) is ordinarily resident in New Zealand; or
>
> (d) in the case of an offence against section 98A, if the group of people in which the person to be charged is alleged to have participated are alleged to have as their objective or one of their objectives the obtaining of material benefits by the commission in New Zealand of offences or conduct referred to in paragraph (a) or paragraph (b) of section 98A(2).

These provisions contain some additional grounds for extending jurisdiction, but a strong link to New Zealand is still required – usually a New Zealand citizen or resident as the actor, or an occurrence on a New Zealand ship or aircraft. This is a relatively traditional approach.

The Terrorism Suppression Amendment Act 2003 made some changes to this. In addition to the provision of offences involving the use and movement of unmarked plastic explosives, and the physical protection of nuclear material – and the other specific offences – the Amendment Act 2003 provides for extraterritorial jurisdiction, extradition, and mutual-assistance requirements in respect of those offences. This is provided for by amendments to section 7 of the Crimes Act 1961. Section 7A lists certain provisions under which prosecution may occur although the acts took place overseas. Previously these have related largely to corruption. The amendment greatly extended the extraterritorial application of the Crimes Act, for it will allow proceedings to be brought for any offence against the Crimes Act committed in the course of carrying out a terrorist act anywhere in the world, provided there is some connection with New Zealand.

---

[37] These offences are: s. 98A of the Crimes Act 1961 (NZ) (participation in organised criminal group), s. 98C (smuggling migrants), s. 98D (trafficking in people by means of coercion or deception), s. 100 (judicial corruption), s. 101 (bribery of judicial officer), s. 102 (corruption and bribery of Minister of Crown), s. 103 (corruption and bribery of Minister of Parliament), s. 104 (corruption and bribery of law-enforcement officer), s. 105(2) (corruption and bribery of official), s. 116 (conspiring to defeat justice), s. 117 (corrupting juries and witnesses), and s. 257A (money laundering), s. 298A (causing disease and sickness in animals), s. 298B (contaminating food, crops, water and other products). Nothing in s. A(1)-(3) of the Crimes Act 1961 (NZ) limits or affects the application of s. 7 to the occurrence in New Zealand of an act or omission forming part of an offence or an event necessary to the completion of an offence: s. 7A(4), as inserted by the Crimes Amendment Act 2002 (NZ), s. 4.

New Zealand courts have jurisdiction over offences in the Terrorism Suppression Act 2002 which occur wholly outside New Zealand if committed by New Zealanders, or against New Zealand property, against New Zealand facilities or citizens, or 'in an attempt to compel the Government of New Zealand to do or abstain from doing any act',[38] or by individuals present in New Zealand and not extradited. The New Zealand courts have jurisdiction if the acts occurred in New Zealand, by the Terrorism Suppression Act 2002, in compliance with the terrorism conventions New Zealand undertook to implement.[39] Under these conventions, other member states also have jurisdiction over acts in New Zealand.

New Zealand law thus asserts extraterritorial jurisdiction in four distinct areas: for crimes on ships and aircraft beyond New Zealand; for crimes committed by people serving New Zealand overseas who are protected by diplomatic immunity; in respect of certain offences with transnational aspects[40] – now including terrorism; and for crimes committed by a New Zealand citizen, corporation, or resident, or by someone found in New Zealand who has not been extradited. There is no general provision for Internet jurisdiction, the Internet being regarded as essentially similar to other telecommunications media.

Section 18 of the Terrorism Suppression Act 2002 was also amended to provide that the principal offences (bombing, financing, or nuclear materials offences) also apply to acts outside New Zealand if the alleged offender is in New Zealand and not extradited. Some, if not all, of these offences may be committed through computer-based communications and data-processing systems.

Where a person does, or omits to do, anything, and is subject to the extraterritorial jurisdiction of New Zealand Courts, that person may be charged with a crime in New Zealand if the act or omission would be a crime if committed in New Zealand.[41] The person will have a defence if the act or omission occurred in the country of which he or she is a citizen or national and it can be shown that that act or omission did not constitute an offence under the law of the country at that time.[42]

There are also other specific extraterritorial provisions which may be relevant to computer crime. Section 144A of the Crimes Act 1961 gives New Zealand Courts jurisdiction in relation to any offences committed outside New Zealand, in that it 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. Though in a

---

[38] Ss. 16(a) and 17(d).

[39] The International Convention for the Suppression of Terrorist Bombings (New York, 15 December 1997; No 37517, UN Doc. A/RES/52/164, Terrorism Suppression Act 2002, Schedule 1); The International Convention for the Suppression of the Financing of Terrorism (New York, 15 December 1997; No 38349, UN GA Resolution A/RES/54/109; Terrorism Suppression Act 2002 (NZ), Schedule 2); as well as the United Nations Security Council (Anti-Terrorism) Resolution 1373 (2001), adopted on 28 September 2001, Reproduced in the Terrorism Suppression Act 2002 (NZ), Schedule 4.

[40] Crimes Act 1961 (NZ), ss. 8, 8A, and s. 7A (as inserted by the Crimes Amendment Act 2002 (NZ), s. 4). Jurisdiction over offences committed by those serving New Zealand overseas was added by the Foreign Affairs and Overseas Service Act 1983 (NZ) and applies to any offences punishable by one year's imprisonment or more, whether or not the act or omission is an offence in the place where it is committed.

[41] Crimes Act 1961 (NZ), s. 8(2).

[42] S. 8(2).

somewhat different context, this might be utilised to give the courts jurisdiction in certain types of cybercrimes.

In general, although New Zealand may have jurisdiction over cybercrimes, it will rarely prosecute unless the offenders are physically located in New Zealand. In some cases this is due to the limited resources of the investigatory agencies. Terrorist offences may prove to be an exception, but no instance of such a crime have yet been prosecuted.

14.3.2. Case Law

There is no New Zealand authority which considers the issue of jurisdiction in a case of international computer misuse. Where a person situated overseas commits an offence involving a computer in New Zealand, or where access is gained by a hacker in New Zealand, the Law Commission considered it likely that New Zealand courts would assume jurisdiction.[43] There is some case law to support this conclusion.

In *Solicitor-General* v. *Reid*,[44] where the respondent had sworn a false affidavit in New Zealand for use in proceedings in the Hong Kong Court of Appeal in return for $1m, Paterson J expressly approved the Canadian decision in *Libman* v. *R*,[45] where it was held by the Supreme Court of Canada that the test was whether there was a 'real and substantial link' between the offence and the country asserting jurisdiction to try the offence. Paterson J stated that had he been required to determine the issue, he would have held that New Zealand courts had jurisdiction to hear the case. He also held that there was nothing contrary to international comity in such an assumption of jurisdiction.

It might also be expected that New Zealand courts would follow the approach taken in *R* v. *Governor of Brixton Prison, ex parte Levin*,[46] where the Court of Appeal of England and Wales held that '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.' This is consistent with *Solicitor-General* v. *Reid*.[47] It is likely that the New Zealand courts will assume jurisdiction when a person situated overseas commits an offence involving a computer in New Zealand, or when the hacker is situated in New Zealand.

The New Zealand Law Commission[48] stated that in its view, section 7 of the Crimes Act 1961 was inadequate to deal with computer misuse. It was anticipated that there would be situations where the effects of computer misuse would be felt in New Zealand, even though neither the hacker nor the computer were situated in this country. The Law Commission gives the example of a hacker in New York, the computer in California, and the owner of the computer

---

[43] New Zealand Law Commission, *Computer Misuse*, Report 54 (Wellington, New Zealand Law Commission 1999), at para. 86.
[44] [1997] 3 NZLR 617 (HC).
[45] (1985) 21 CCC (3d) 206 (SCC).
[46] [1997] QB 65, 82 (CA).
[47] [1997] 3 NZLR 617 (HC).
[48] New Zealand Law Commission, op. cit. n. 43, at para. 86.

system in New Zealand.[49] In such a situation section 7 would not give jurisdiction, unless it was a terrorism-linked offence.

It might be impossible to successfully argue, in terms of section 7 of the 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. The words 'necessary to completion of the offence' in this context have been held to relate to the completion of the legal ingredients, not the offender's purpose[50] – unless it was terrorism.

In many cases it would be impossible to determine where the hacker was at the time the computer misuse activities took place.[51] However, the 2003 amendments to the Crimes Act 1961 extended jurisdiction to events occurring wholly outside New Zealand where the offence was committed in the course of carrying out a terrorist act, and several other specific offences.

14.4. Policy Considerations

14.4.1. Claiming Jurisdiction for Cybercrimes

Historically, there has been a legislative presumption against the extraterritorial application of public-law statutes, as a matter of statutory interpretation.[52] This is based on an historical concern not to infringe on the sovereignty of other states (or provinces) by purporting to regulate conduct that occurs wholly within the boundaries of another jurisdiction.[53] Customary international law however permits a nation to apply its law to extraterritorial behaviour with substantial local effect,[54] as well as the extraterritorial conduct of its citizens or domiciliaries.[55] Until very recently, New Zealand law reflected this narrow exemption. Even where an assertion is not aggressive there can be overlapping claims to jurisdiction.

In *Libman*,[56] the Supreme Court of Canada ruled that 'it is sufficient that there be a "real and substantial link"' between the proscribed conduct and the jurisdiction seeking to apply and enforce its law. Clearly, the 'real and substantial link' test for the proper assertion of prescriptive jurisdiction will often result in more than one, and perhaps many, jurisdictions being capable of properly asserting authority over conduct that has effects in more than one jurisdiction. It is this fact that suggests the need for clearer prescriptive

---

[49] New Zealand Law Commission, op. cit. n. 43, at para. 86n.

[50] See *Collector of Customs* v. *Kozanic* (1983) 1 CRNZ 135.

[51] New Zealand Law Commission, op. cit. n. 43, at para. 25 gives the example of the *Ihug* case (1998) where the computer was based in California and was owned by a New Zealand company and some 4,500 websites were erased.

[52] Though there are important exceptions, including in the consumer law field. For example, the Fair Trading Act 1986 (NZ) states, in s. 3, that '[t]his Act extends to the engaging in conduct outside New Zealand by any person resident or carrying on business in New Zealand to the extent that such conduct relates to the supply of goods or services, or the granting of interests in land, within New Zealand.'

[53] R. Tassé and M. Faille, 'Online Consumer Protection in Canada: The Problem of Regulatory Jurisdiction', 2 *Internet and E-Commerce Law in Canada* (2000/01) p. 41. See also *Buchanan* v. *Rucker* (1808) 9 East 192; 103 ER 546, 547: 'Can the Island of Tobago pass a law to bind the rights of the whole world?'

[54] The case of the 'SS Lotus', 1927 PCIJ (ser. A) No 10, 18-25. Cf., section 5.6.1 of this book.

[55] *Blackmer* v. *US*, 284 US 421, 436 (1932); *US* v. *Rech*, 780 F2d 1541, 1543 n 2 (11th cir, 1986).

[56] *R* v. *Libman* [1985] 2 SCR 178.

jurisdictional rules,[57] especially for consumer laws. In *Dow Jones & Company Inc* v. *Gutnick*,[58] the High Court of Australia found that certain categories of laws did have extraterritorial effect, and certain laws in New Zealand, such as the Consumer Guarantees Act 1993, have been held to have extraterritorial effect. Competing claims to jurisdiction do not necessarily mean that all cases will be prosecuted, however.

The difficulty facing national jurisdictions is one of enforcement, which has led to other forms of regulation, including (but not limited to) trans-national, international, institutional, sectoral and private.[59] There are an increasing number of examples of private control or self-regulatory control, sometimes involving codes. Unfortunately these disparate approaches exasperate the already marked divisions. Nor are there signs that international co-operation will be practical outside narrow legal fields such as copyright and cybercrime,[60] even if it is effective there.

Hacking, or the unauthorised access to computer systems, is one aspect of cybercrime which might legitimately be within the jurisdiction of all states – especially if the hacking is malicious, but even when not. As Paterson J observed in *Solicitor-General* v. *Reid*,[61]

> There was a real and substantial link between the offence under (…) the Crimes Act and New Zealand. International comity 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 [causes] harm (...) in another country.[62]

Hacking is not confined to a single geographical location; by its very nature, it involves the invasion of computer systems physically remote from the offender. For this reason alone, and because of the damage which may occur through damage to systems or data, or through the release of information, jurisdictional considerations ought not to be allowed to inhibit the successful detection, prosecution and conviction of offenders.

If this is true of hacking, it is doubly so for the creation, release and dissemination of computer viruses. With the growth of Internet and email communications across the world it is possible for a virus, whether benign or malignant, to spread extremely rapidly. It is especially dangerous because the degree of security customarily found in computer systems varies markedly around the world. While the traditional early sources of computer viruses included New Zealand, more recently, the sources of virus infections have spread to countries with even less well-developed legal responses to cybercrime. For this reason, and since damage may occur anywhere a virus can reach (which is effectively global reach), criminal jurisdiction should be asserted as widely as possible.

---

[57] Tassé and Faille, loc. cit. n. 53.

[58] (2002) 194 ALR 433 (HCA).

[59] See, for example, L. Lessig, *Code and other laws of cyberspace* (New York, Basic Books 1999); C. Marsden, *Regulating the Global Information Society* (London, Routledge 2000).

[60] See the Copyright Treaty of the World Intellectual Property Organisation, adopted in Geneva on December 20, 1996, and the Council of Europe's Convention on Cybercrime, Budapest, November 23, 2001 (CETS 185).

[61] [1997] 3 NZLR 617, 630, 632.

[62] *Solicitor-General* v. *Reid* [1997] 3 NZLR 617, 630, 632 per Paterson J, *Treacy* v. *Director of Public Prosecutions* [1971] AC 537; [1971] 1 All ER 110 per Lord Diplock at 561-562/121-122 and *Libman* v. *The Queen* [1985] 2 SCR 178; (1985) 21 CCC (3d) 206 followed.

Similar arguments apply with respect to the control of on-line illegal content. Harmful content may be accessed anywhere in the world, and the originator of the content may not even be locatable, since the material may pass from website to website by copying or file-sharing, or from email user to email user in the manner of a chain letter, or as 'spam'.

However, the regulation of content also involves consideration of culture-specific values. It may be relatively easy to identify a website or email that offends against a specific domestic law, but the process involved in searching for these offences may amount to a form of censorship. Indeed, though it is quite possible to censor the content of the Internet, it is possible that its continuing expansion will render this option increasingly difficult. But it remains vital that some claims to jurisdiction are made. The United States position is that even if a foreign court passes a judgment or direction against a legal entity of a particular country, say country A, then that judgment or direction would not be applicable automatically to country A's legal entity or citizen.[63] In the numerous international judgements since the advent of the Internet, some courts have simply applied traditional jurisdictional rules,[64] while others have tried to devise new tests to accommodate the peculiarity of the medium.[65] This has caused uncertainty and difficulties for courts, and sometimes possibly led to illegal content being published and spread more than it would have been if jurisdictional claims had been clearer.

The general rule governing criminal jurisdiction in New Zealand is that nothing done or omitted outside New Zealand can be tried in New Zealand as an offence, unless statutes specifically provide otherwise.[66] However, New Zealand law asserts extraterritorial jurisdiction in respect of certain offences with transnational aspects.[67] Proceedings under these specified offences may also be brought if a person in respect of whom the offences alleged to have been committed is a New Zealand citizen, or is ordinarily resident in New Zealand.[68] Proceedings may also be brought for an offence against section 98A of the Crimes Act 1961 (participation in an organised criminal gang), if the group of people in which the person to be charged is alleged to have participated are alleged to have as an objective the obtaining of material benefits by the commission in New Zealand of offences or conduct referred to in section 98A(2)(a) or (b). Both of these provisions may apply to cybercrimes. These are applied to terrorism and certain specific crimes, especially organised crime and corruption, but have no general application.

---

[63] *Yahoo! Inc* v. *La Ligue contre Le Racisme et L'Antisemitisme*, 145 F Supp 2d 1168; 169 F Supp 2d 1181 (2001); A. Manolopoulos, 'Raising 'Cyber-Borders': The Interaction Between Law and Technology', 11 *International Journal of Law and Information Technology* (2003) p. 40.

[64] Such as *Bensusan Restaurant Corp. v. King*, 40 USPQ (2d) 1519 (SDNY), confirmed by United States Court of Appeals (2d cir) 10 September 1997.

[65] See O. Renault, 'Jurisdiction and the Internet: Are the traditional rules enough?', paper prepared by the Uniform Law Conference of Canada (1998), available at http://www.law.ualberta.ca/alri/ulc/current/ejurisd.htm.

[66] S. 6 Crimes Act 1961 (NZ). This enacts the common law principle that statutes are not to be construed as giving extraterritorial jurisdiction unless there are clear words to that effect, as to which see *Macleod* v. *Attorney-General for New South Wales* [1891] AC 455 (PC). The general rule that 'all crime is local' was repeated by the Court of Appeal in *R* v. *Sanders* [1984] 1 NZLR 636; (1984) 1 CRNZ 194 (CA).

[67] See *supra*, section 14.3.1 and note 40.

[68] Crimes Act 1961 (NZ), s. 7A(1)(c)(i) and (ii), as inserted by the Crimes Amendment Act 2002 (NZ), s. 4.

The assertion of extraterritorial jurisdiction may be justified as based on a state's responsibility for the actions of its people, wherever situated. A general assertion of jurisdiction would be seen to be contrary to the notion of the sanctity of state sovereignty. But, as we have seen, this self-imposed limitation has been weakened with respect to terrorism offences.

14.4.2. Dealing with Cyber-Investigation Jurisdiction

This problem of jurisdiction is not unique to New Zealand, or the Asia Pacific region, or elsewhere – though countries such as New Zealand are particularly vulnerable as they are small and geographically remote from major trading partners, and therefore major potential users of the Internet.

Law-enforcement co-operation with foreign counterparts is critically important to United States efforts (in particular) to address the challenges of cross-border Internet fraud. The same technology that Internet frauds use is proving invaluable to international law enforcers whose job is to track down fraudsters and stop their activities. This is achieved by identifying non-complying websites, and informing them that they are acting illegally. Only as a last resort is legal action undertaken. The United States' Federal Trade Commission (FTC) also plays an active role in public policy discussions on international consumer-protection principles for the global economy.[69] New Zealand has also relied heavily on international co-operation.

New Zealand and other countries cannot investigate crimes without reliance on international co-operation. Cybercrime generally (though not invariably) occurs across jurisdictional boundaries – or at least is often oblivious to jurisdictions. This situation requires a balanced approach of 'co-regulation', or what has been called 'a new paradigm for governance that recognizes the complexity of networks, builds constructive relationships among the various participants (including governments, systems operators, information providers, and citizens), and promotes incentives for the attainment of various public policy objectives in the private sector.'[70]

Proper enforcement of such applicable criminal laws as exist requires effective investigatory powers. These powers need to be grounded in technology-neutral legislation, which will not become outmoded as computer technology advances. For example, police require authority to conduct network searches, just as they require authority to conduct physical searches. It is unsatisfactory that the current legislative provisions in New Zealand are not clear – except perhaps with respect to the rather more specific powers conferred upon the Police with respect to investigating terrorist activities. If evidence of criminal offending were to be gathered through police searches of computer networks, it is not even certain that this evidence would be usable in a prosecution.

While the power to authorise the interception of telecommunications is vital for the preservation of national security, it is also a useful, indeed invaluable,

---

[69] J. Bernstein, Director, Bureau of Consumer Protection, U.S. Federal Trade Commission, 'Fighting Internet Fraud: A Global Effort', *Economic Perspectives, An Electronic Journal of the United States Department of State*, 5 (May 2000), available at http://usinfo.state.gov/journals/ites/0500/ijee/ftc2.htm.

[70] J.R. Reidenberg, 'Governing Networks and Rule-Making in Cyberspace', in B. Kahin and C. Nesson, eds., *Borders in Cyberspace* (Cambridge, MIT Press 1997), pp. 84-105

tool for the detection of crime, including cybercrime. However, unlike authorising the searching of computers where suspicion of offending has arisen, there is a danger that a too-wide right to intercept telecommunications might be used rather as a 'fishing net', in the hope of discovering something of interest. The consequence for the great majority of users of telecommunications is that their privacy is infringed – generally without their knowledge, and always without their consent. The investigatory powers of interception need careful control, therefore, especially where this information may be passed on to other countries, or where the interception is at the behest of another country.

There is much greater justification for allowing the infiltrating of on-line child-pornography networks. Although there are difficulties of definition and degrees of offending, this sort of material is generally relatively readily identified as offensive. It also is very frequently international in scope, with vice-rings creating, swapping and collecting material from multiple sources. It is often this very internationality which renders the detection and prosecution of offenders difficult. There have already been many examples of international police operations aimed at disrupting these large-scale offenders, which have often been very effective, for a time. However, the scale of the problem is such that it cannot be tackled by any single country or small groups of countries, and would be more effectively dealt with as simply another form of offence for the national authorities to deal with. This requires the existence and exercise of jurisdiction in all countries where the Internet operates – for it is not reliant on the existence of Internet Service Providers.

14.4.3. Positive and Negative Jurisdiction Conflicts

Given that most cybercrimes are agreed to be criminal offending and worthy of punishment, but that criminal law is domestic and not international in nature, one of the biggest dangers is that some instances of this offending escape prosecution because of a failure to prosecute, or the failure of a prosecution due to jurisdictional or evidentiary difficulties. Extradition of offenders from one country to another is not practical except in a few instances – and even this requires that the offence is criminal in both countries.[71] In the absence of an international police agency empowered to investigate and prosecute before domestic or international courts, the best solution may well be a gradual process of consolidating and standardising laws, both criminal and procedural. This would not only reduce the chances of a failure in prosecution, but would also assist those countries that have less well-developed technology laws.

Another potential danger however is a conflict of jurisdictions, where multiple countries claim jurisdiction over an offence. This not only raises the danger of protracted trials and litigation, but also offers the possibility of over-criminalising activities and creating situations where double jeopardy may arise. Even the existence of multiple individual claims does not guarantee that a single prosecution will occur. Again, gradual standardisation would help to reduce these possibilities.

As an initial step, co-operative agreements between policing agencies should be utilised. Much can be done without the necessity of legislation enactments,

[71] This is the rule, though there are exceptions.

for there is a considerable degree of investigative discretion in most countries, and many investigative powers which are common. This may proceed as bilateral and multilateral agreements, but ideally should include international conventions. Conventions such as the Budapest Convention on Cybercrime would be strengthened and their effectiveness greatly enhanced if appropriate administrative and investigative procedures and processes existed.

14.5. Conclusion

New Zealand has still not fully addressed the jurisdictional issues that cybercrime raise. There is no single assertion of jurisdiction. Even if this were made, it is doubtful that jurisdiction would be sought or exercised in practice. New Zealand, largely for reasons of limited resources, does not take an especially pro-active role. While it co-operates with the law-enforcement agencies of other countries, its own ability to combat cybercrime is reduced by lingering uncertainty regarding the nature of the electronic media – concerns only partly allayed by recent legislative changes.

Pragmatism and a lingering belief in the notion of state sovereignty have prevented a wide assertion of extraterritorial jurisdiction over cybercrime. The former is in recognition of the limited practical scope for discovering, prosecuting and punishing offences committed overseas. The latter is perhaps due to a strong sense of individualism, a less well-developed sense of national comity, and continued support for the post-Westphalian notion of jurisdictional sovereignty.

If all states were to have jurisdiction over cybercrimes – and were to exercise that – and domestic laws were made consistent with one another, there could be a gradual move towards the development of an international customary law. This could reconcile both the concept of state sovereignty and the need to ensure that cybercrimes are prosecuted efficiently and properly.

Bibliography

J. Bernstein, 'Fighting Internet Fraud: A Global Effort', *Economic Perspectives, An Electronic Journal of the United States Department of State* (May 2000), http://usinfo.state.gov/journals/ites/0500/ijee/ftc2.htm.

D. Harvey, *Internet.law.nz: selected issues* (Wellington, LexisNexis, 2003)

A. Manolopoulos, 'Raising 'Cyber-Borders': The Interaction Between Law and Technology', 11 *International Journal of Law and Information Technology* (2003) p. 40.

P. Myburgh & E. Schoeman, 'Jurisdiction in trans-national cases', *New Zealand Law Journal* (2004) p. 403.

New Zealand Law Commission, *Computer Misuse*, Report 54 (Wellington, New Zealand Law Commission 1999)

O. Renault, 'Jurisdiction and the Internet: Are the traditional rules enough?', paper prepared by the Uniform Law Conference of Canada (1998), available at http://www.law.ualberta.ca/alri/ulc/current/ejurisd.htm.

J.R. Reidenberg, 'Governing Networks and Rule-Making in Cyberspace', in B. Kahin and C. Nesson, eds., *Borders in Cyberspace* (Cambridge, MIT Press 1997).

T. Smith, 'Fighting on the ocean blue: New Zealand's extra-territorial jurisdiction and maritime protest', 32 *Victoria University of Wellington Law Review* (2001) p. 499.

R. Tassé and M. Faille, 'Online Consumer Protection in Canada: The Problem of Regulatory Jurisdiction', 2 *Internet and E-Commerce Law in Canada* (2000/01).