A Patch On The System? E-Crime and the Crimes Amendment Act 2003

Anthony Trenwith*

I: Introduction

1. Overview

New Zealand's recent e-crime legislation, the Crimes Amendment Act 2003 ("the Act"), brings it into line with much of the rest of the developed world.[1] However, the new legislation raises more issues than it resolves, and consigns many of these issues to resolution by the courts. Early cases argued under the new legislation are likely to be hard cases making for bad law. The courts will probably take some time to define clearly the Act's broad and indistinct boundaries, delineate between the innocuous and the criminal, and thus determine an answer to the question: "what is an e-crime?" Therefore, the hypothesis of this article is that the new legislation is merely a 'patch on the system', filling a pre-existing lacuna in the law, but failing to provide any detailed guidance for those involved in deciding e-crimes cases. This article does not undertake a comparative analysis of e-crime legislation from different jurisdictions. Rather, it focuses on the New Zealand Act, making reference to provisions in, and cases decided under, comparable legislation, with a view to indicating how cases involving New Zealand's e-crime legislation might be decided.

The first part of the article examines the issue of jurisdiction, a key aspect of any e-crime case given the global nature of today's information age. It draws upon New Zealand precedents involving jurisdictional issues, as well as judgments from the United Kingdom and United States, in order to glean guidance on how New Zealand courts might approach the extraterritorial nature of e-crime.

The second part is a comprehensive and in-depth analysis of the main e-crime provisions in the Act: sections 248 to 252.[2] The third part considers future developments regarding prosecutorial issues in e-crimes. Finally, the article

---

* BA/LLB. I would like to thank Judge David Harvey, Faculty of Law, University of Auckland, for his invaluable assistance; Duncan Gardiner of the New Zealand Police E-Crime Laboratory in Auckland for his time and input; and my brother John Trenwith for knowing the things that I did not.

1 For a list of 44 countries with specific e-crime laws see Schjolberg, "The Legal Framework - Unauthorized Access To Computer Systems", *Moss District Court*, 7 April 2003 <http://www.mosstingrett.no/info/legal.html> (at 11 July 2004).

2 Sections 253 and 254, which provide qualified exemptions to the preceding sections for the New Zealand Secret Intelligence Service and the Government Communications Security Bureau, are not discussed.

concludes by reviewing anomalies identified in the legislation, and by passing a verdict on its anticipated functionality in practice.

2. Crime and the Information Age – Making the Intangible Intelligible

The overall purpose of any e-crime legislation is to align the law with contemporary society, allowing it to keep pace with societal changes and remain an effective enforcement tool. In New Zealand, considerable social change has taken place since the original enactment of the Crimes Act 1961. Consequently the legislation has struggled to keep pace with new concepts of property – as well as new forms of criminal activity involving these new concepts of property – that were virtually unknown when the Crimes Act 1961 was passed.[3]

One example of this is the phenomenon of "hacking".[4] Some 20 years after the first hackers, the 1983 movie War Games introduced the concept into popular culture and public consciousness.[5] In the wake of this film and subsequent hacking activity, the United States Government passed the Computer Fraud and Abuse Act 1986 (US). Four years later, the United Kingdom followed suit with its Computer Misuse Act 1990 (UK). In New Zealand, deficiencies caused by the absence of a similar Act were highlighted by several e-crime incidents.

The first, in November 1998, resulted in 4,000 files being deleted from Internet Service Provider ("ISP") Ihug's homepages server situated in California.[6] Investigations revealed that a 17-year-old New Zealander was responsible,[7] yet no charges were laid. However, it was reported that Ihug considered extraditing the hacker to the United States, as New Zealand law was "inadequate to deal with cyber-vandalism".[8]

Mere months after that incident, another ISP, Xtra, was the victim of a similar attack: a "Trojan Horse" program was used to gain remote access to at least

3 Although the development of hacking has essentially been contemporaneous with that of computers, the term first began to be used in 1961 at Massachusetts Institute of Technology. See "Hacking's History" *PCWorld.com*, 10 April 2001 <http://www.pcworld.com/news/ article/0,aid,45764,00.asp> (at 11 July 2004).

4 A distinction is commonly drawn between "hackers", who access systems without malicious intent, and "crackers" who access systems with such intent. For convenience, the term "hacker" is used generically throughout this paper to cover both terms.

5 Calkins, "They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models" (2000) 89(1) Geo LJ 171, 179. See also DeMarco, "It's Not Just Fun and 'War Games' – Juveniles and Computer Crime", *US Attorneys' Bulletin*, May 2001 <http://www.usdoj.gov/criminal/cybercrime/ usamay2001_7.htm> (at 11 July 2004).

6 "Ihug boosts security after hacker hits 100 accounts", *The New Zealand Herald*, Auckland, New Zealand, 1 February 2000, <http://www.nzherald.co.nz/storydisplay.cfm?storyID= 114894> (at 11 July 2004).

7 Harvey, *internet.law.nz* (Wellington, 2003), 174-175.

8 "Teenage hacker faces extradition bid", *The Dominion*, Wellington, New Zealand, 21 November 1998 (Edition 2), 10.

200 passwords from Xtra customers.[9] The Xtra hacker was prosecuted in what became one of New Zealand's first e-crime cases.[10] However, the nature of the prosecution itself was problematic. Due to an earlier Court of Appeal ruling that intangible property was not legally capable of being stolen[11] the defendant could not be charged with theft. Instead he was charged with wilful damage.[12] That charge was based on an English case (prior to the introduction of the Computer Misuse Act 1990 (UK)) in which the argument that wilful damage resulted from "alteration to magnetic particles on the disk" was used in a successful prosecution for hacking.[13] Contrived though the argument was, it was nonetheless equally successful in New Zealand (although the jury disagreed as to a verdict), and was used again in 2003.[14]

Ultimately, the wilful damage approach was always going to be limited in its application. It is a crude cousin to more technologically appropriate approaches – such as those contained in the new Act – and also requires both court and counsel to engage in something akin to a game of The Emperor's New Clothes. Hence the need for the long overdue law change brought about by the new Act.

II: Jurisdiction – My Place Or Yours?

1. The New Zealand Approach

In any attempt to establish a legal framework for e-crime, jurisdiction will always be one issue that is fraught with difficulty. The Internet crosses geographical and political borders without regard for jurisdiction. Therefore, because of the very nature of such technology, e-crime will almost inevitably surpass jurisdictional boundaries. New Zealand is fortunate to have a single, national jurisdiction. However, "discrete" e-crime cases (those confined exclusively to New Zealand) are likely to be the exception, rather than the rule. How, then, should jurisdictional issues in e-crime cases be resolved?

The general rule governing criminal jurisdiction in New Zealand is that nothing done (or omitted) outside New Zealand can be tried as an offence in New Zealand.[15] The rule is based on the common law principle that statutes are not to be construed as giving extraterritorial jurisdiction unless there are clear words to that effect.[16] As Lord Halsbury said in *Macleod v Attorney-General for New*

9 "Hacked off at the way it all played out", *The New Zealand Herald*, Auckland, New Zealand, 1 September 2001 <http://www.nzherald.co.nz/storydisplay.cfm?storyID=213042> (at 11 July 2004). For an explanation of "Trojan Horse", see III(2)(a) below.

10 *R v Garrett* [2001] DCR 955.

11 *R v Wilkinson* [1999] 1 NZLR 403.

12 Supra note 10, 977.

13 *R v Whiteley* (1991) 93 Cr App R 25 (CA).

14 See "Hacker admits wilful damage" *The New Zealand Herald*, Auckland, New Zealand, 25 February 2003, <http://www.nzherald.co.nz/storydisplay.cfm?storyID=3197605> (at 11 July 2004).

15 Crimes Act 1961, s 6.

16 *Macleod v Attorney-General for New South Wales* [1891] AC 455 (PC).

South Wales: "All crime is local. The jurisdiction over the crime belongs to the country where the crime is committed".[17] This is however subject to section 7 of the Crimes Act 1961, which states:

> **7. Place of commission of offence—**
> For the purpose of jurisdiction, where any act or omission forming part of any offence, or any event necessary to the completion of any offence, occurs in New Zealand, the offence shall be deemed to be committed in New Zealand, whether the person charged with the offence was in New Zealand or not at the time of the act, omission, or event.

A number of cases provide guidance on how this section is to be applied. One example is the judgment of Roper J in *Collector of Customs v Kozanic:*[18]

> [T]he "act or omission" [in section 7] refers to the acts or omissions which together comprise the actus reus of the offence; and the "event" refers to any happening which is necessary to make the offence complete. Not every offence or crime requires both "an act forming part" and "an event necessary to completion".

His Honour included in his decision the proviso that the stated conclusions were given "'in the circumstances of this case'".[19] The application of section 7 was again considered the following year in *R v Sanders*.[20] In *R v Sanders*, the Court of Appeal, while not referring to the decision in *Collector of Customs v Kozanic*, held that the New Zealand courts have jurisdiction to try cases involving conspiracies entered into outside of New Zealand's territorial jurisdiction but implemented in New Zealand. McMullin J delivered the judgment of the Court:[21]

> [I]t is noteworthy that the very words of s 7 ... contemplate that not all acts or omissions forming part of the offence need be committed in New Zealand; some, perhaps almost all, may occur outside. It is sufficient if one act or omission forming part of the offence or "any event necessary to the completion of any offence" occurs in New Zealand. In the use of these words s 7 effectively recognises that the ingredients of a crime may be satisfied by activity which continues on from some earlier starting point.

Two years later the Court of Appeal affirmed their earlier decision, holding that the use of the New Zealand Customs and Postal Services in the performance of a continuing conspiracy brought an offence within the jurisdiction of the New Zealand courts.[22]

---

17 [1891] AC 455, 458 (PC).
18 (1983) 1 CRNZ 135, 138.
19 Ibid 139.
20 [1984] 1 NZLR 636 (CA).
21 Ibid 639-640.
22 *R v Johnston* (1986) 2 CRNZ 289. See also *Solicitor-General v Reid* [1997] 3 NZLR 617.

2. Comparison with International Approaches

In *R v Governor of Brixton Prison, ex parte Levin*,[23] the English Court of Appeal held, in the course of extradition proceedings, that Levin could have committed theft in the United States by fraudulently accessing a computer operated by Citibank in Parsippany, New Jersey, even though he had been sitting at his computer in St Petersburg, Russia, the whole time.[24] Beldam LJ gave the decision of the Court:[25]

> [I]n the present case, no instructions [concerning the transfer of the stolen funds] could be given without first gaining entry into the Citibank computer in Parsipenny. ... We see no reason why the appropriation of the client's right to give instructions should not be regarded as having taken place in [that] computer. ... The fact that the applicant was physically in St Petersburg is of far less significance than the fact that he was looking at and operating on magnetic disks located in Parsipenny. The essence of what he was doing was done there.

This decision was reached according to the English approach to territorial jurisdiction, which, unlike the New Zealand view, is based on common law and not on statute.[26] Nevertheless, the cases cited above show that a similar result could be reached in New Zealand by applying section 7.

Furthermore, the principle could be applied two ways: to acts initiated in New Zealand but completed overseas, and also to acts initiated overseas but completed in New Zealand. For example, a person in New Zealand who used a Trojan Horse or virus to gain control of another computer overseas could be charged with having committed an offence under section 251. The rationale behind this is as follows: in the former example, the sending of the virus or Trojan Horse was an event necessary to the completion of an offence, while the sending of the commands required to take control of the other computer system was an event necessary to the completion of an offence under section 251. In the inverse situation, where the offence was initiated overseas, New Zealand courts could claim jurisdiction on the grounds that unauthorized access was gained, or damage done, to a computer system physically located in New Zealand, or that a New Zealand company suffered financial loss as a result of the unauthorized access. If a New Zealand ISP was used, the courts could claim jurisdiction on similar grounds to those expressed in *R v Johnston*.[27]

---

23 [1997] QB 65.

24 Hirst, "Cyberobscenity and the Ambit of English Criminal Law" 13(2) Computers & the Law 25 June/July 2002.

25 Supra note 23, 81-82.

26 *Director of Public Prosecutions v Stonehouse* [1978] AC 55 (HL). See also *Libman v The Queen* (1985) 21 CCC (3d) 206, 232 (SCC), where the test was held to be "a real and substantial link" to overcome the Canadian equivalent of s 6 of the Crimes Act 1961 (NZ). Canada has no equivalent to s 7.

27 Supra note 22.

Ultimately then, although it is as yet untested, it seems that section 7 provides the New Zealand courts with considerable flexibility to bring a case within their jurisdiction through the recognition of "initiatory" as well as "terminatory" jurisdiction.[28] Thus, even where jurisdiction cannot be automatically inferred from the physical location of the servers or individual concerned, the courts can assume jurisdiction, as long as a domestic connection still exists.[29] Natasha Jarvie discusses this issue:[30]

> A further characteristic of the internet, which challenges effective detection and prosecution, is that many internet transactions involve more than one – and often several – jurisdictions. ... The globalisation of telecommunications enhances the ability of offenders to ... transcend national boundaries [and obstruct] law enforcement. This additional dimension requires the determination of two questions fundamental to the successful prosecution of the offender. First, where was the offence committed, and second what evidence is available to prosecute the offender before a court?

As Jarvie notes, courts have addressed similar issues in the past. She gives the example of *US v Thomas*,[31] in which "the defendants operated a computer bulletin board, allowing subscribers to download pornographic images".[32] The material in question was considered lawful in California, where the defendants' bulletin board was operated, yet the defendants were guilty of several counts of distributing obscenity via the bulletin board in violation of Federal obscenity laws. On appeal, the Sixth Circuit Court of Appeals held that "venue ... lies 'in any district from, through, or into which' the allegedly obscene material moves".[33] Thomas was also separately indicted in Utah for distribution of pornographic materials via the Internet in that state.[34] His motion to dismiss the Utah indictment on the grounds of double jeopardy arising out of his Tennessee conviction and sentencing was rejected by the Tenth Circuit Court of Appeals. In its decision, the appellate Court adopted the District Court's reasoning:[35]

> [N]one of the images which form the basis of the Utah indictment were the basis of the Tennessee charges, and ... the Tennessee jury made no findings regarding child pornography on the bulletin board .... [T]he Tennessee sentencing judge made no findings with regard to child pornography on Mr. Thomas' bulletin board.

---

28 Williams, "Venue and the Ambit of Criminal Law" (1965) 81 LQR 518, 527.

29 But see New Zealand Law Commission *Computer Misuse: Report 54* (NZLC R54, May 1999) [86]-[87], which considers s 7 to be inadequate and recommends a provision be enacted giving New Zealand universal jurisdiction over e-crime offences. However, the author considers this overkill – hackers are not *hostes humani generis* (enemies of the human race) and the establishment of universal jurisdiction would set a dangerous precedent in a grey area of law. See also Henry Kissinger "The Pitfalls of Universal Jurisdiction" (2001) 80(4) Foreign Affairs 86.

30 Jarvie, "Control of Cybercrime" [2003] CTLR 110, 112.

31 74 F 3d 701 (6th Cir, 1996).

32 Supra note 30, 113.

33 *US v Thomas*, supra note 31, 709.

34 1997 US App LEXIS 12998; 113 F 3d 1247 (table) (10th Cir, 1997).

35 Ibid 3.

The *Thomas* case illustrates the fluidity that results from applying law to the Internet. In *Thomas*, the applicable law was restricted to United States Federal law, because bulletin board systems were, at the time, essentially restricted by the cost of international toll rates. However, the global nature of the Internet now eliminates this barrier; modern equivalents of Thomas's board are opened up to the world, and those who own and operate them are made vulnerable to global prosecution. This in turn creates a number of legal complexities. The amicus brief of the Electronic Frontier Foundation in *Thomas* (1996) gave a warning:[36]

> The precedents we set today may radically affect the course of the computer networks of the future, and with it the fate of an important tool for the exchange of ideas in a democratic society. When the law limits or inhibits the use of new technologies ... it creates a grave risk of compromising ... interests protected by the Bill of Rights.

The respective courts in the *Thomas* cases thus had developed the application of personal jurisdiction to the Internet. The case of *United States v Kammersell*[37] added a twist to the rules. In that case, the defendant sent his girlfriend a bomb threat at work, hoping that it would enable her to leave early and go on a date with him. The threat was sent via the Instant Messenger service produced by America Online ("AOL").[38] While both the defendant and his girlfriend were residing in Utah at the time, all AOL instant messages were automatically sent to AOL's main server in Virginia before proceeding to their final destination.[39] On this basis, the Court found that the message had travelled interstate,[40] thus triggering the jurisdictional requirements of the relevant federal law.[41] This law was last amended in 1939 – when the primary mode of communication was the telephone – leading the defendant to argue for it to be interpreted "in light of the sweeping changes in technology over the past 60 years"; the prosecution urged the Court to adhere to the plain meaning.[42] Although the Court considered the defendant's argument compelling, agreeing that legislative reconsideration of the statute was highly desirable, it held that he could not rely on this argument to escape criminal prosecution where the statutory language literally allowed for such prosecution.[43] Considering both the *Thomas and Kammersell* cases, Eugene Quinn concludes:[44]

---

36 Brief o f amicus curiae, Electronic Frontier Foundation, *US v Thomas*, 74 F.3d 701(1996) (No. 94-6648, 94-6649) <http://www.eff.org/Legal/Cases/AABBS_Thomases_Memphis/eff_aa_ 041995_amicus.brief> (at 11 July 2004).

37 196 F 3d 1137 (10th Cir, 1999). Cert denied June 12, 2000: 530 US 1231.

38 Instant Messenger allows individuals to communicate by typing messages that when sent appear in a pop-up window on the recipients screen. See "About AOL Instant Messenger" <http://www.aim.com/help_faq/starting_out/getstarted.adp?aolp=#whatis> (at 11 July 2004).

39 Supra note 37, 1138.

40 Ibid 1139.

41 18 USC §875(c) – "Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both."

42 Supra note 37, 1139.

43 Ibid.

44 Quinn, "The Evolution of Internet Jurisdiction: What A Long Strange Trip It Has Been" [2000] Syr JL & Tech 1, 56, 60-61, 62.

> Given the increasing flow of Internet communication ... we should consider the need for a retreat from a rule that subjects each and every Internet user to the reach of the federal government simply by using a server located in a foreign state. ... This [rule] is particularly alarming when you recall that a message is divided into packets before it is sent and each packet is transmitted individually. These individual packets can, and often do, follow different routes to the ultimate destination. Once all the packets forming a message arrive at the destination the packets are reassembled into the original message. ... [I]t is conceivable that a message ... may travel around the globe, through countless jurisdictions, prior to being delivered. The problem is that the sender has no control over where the material will travel en route to its ultimate destination. ... Absent a solution to this problem communications over the Internet will be unnecessarily chilled for fear of prosecution in some remote jurisdiction .... [I]f we are challenged by the applicability of something as fundamental as jurisdiction, what surprises lurk for us in the shadows of the Internet?

Quinn's conclusions are particularly relevant to a jurisdiction such as New Zealand, which can potentially exercise "long arm" powers of jurisdiction over almost anyone, anywhere in the world. This in personam jurisdiction is useful when dealing with Internet-related issues, where the application of territorial jurisdiction can be blocked by political and geographical boundaries as well as a lack of "place".[45]

Having considered the issue of jurisdiction, and its application to e-crime laws, the laws themselves will now be subjected to closer scrutiny.

III: Section By Section Analysis

1. Section 248 – Redefining Reality

Section 248 defines major terms that relate to the new offences. Unusually, the definitions only explicitly extend to section 248 and the two subsequent sections. They do not explicitly apply to sections 251, "Making, selling, or distributing or possessing software for committing crime" and 252, "Accessing a computer system without authorisation". It can only be assumed that the definitions in section 248 will apply to sections 251 and 252 by implication.

It is interesting to contrast definitions in the Act with those preferred by the Law Commission in their report "Computer Misuse"[46] (the forerunner to the new legislation), as well as with definitions contained in the original Crimes Bill 1989 ("the Bill"). The Law Commission considered the term "computer" was best left undefined.[47] The definition in the Bill was: "'Computer system' means a

45 See generally Hunter, "Cyberspace as Place and the Tragedy of the Digital Anticommons" (2003) 91 CLR 439.

46 New Zealand Law Commission, supra note 29.

47 Ibid [15].

set of related computer equipment, devices, and software, whether connected or unconnected to one another."[48] The enacted definition reads:

> **computer system—**
> (a) means—
> (i) a computer; or
> (ii) 2 or more interconnected computers; or
> (iii) any communication links between computers or to remote terminals or another device; or
> (iv) 2 or more interconnected computers combined with any communication links between computers or to remote terminals or any other device; and
> (b) includes any part of the items described in paragraph (a) and all related input, output, processing, storage, software, or communications facilities, and stored data.

The new definition is significantly more complex than previously proposed. However, it is not more precise. This is due, in part, to the omission of the word "related", which appeared in the 1989 Bill but not in the Act. By removing the requirement for multiple computers to be related, and requiring them only to be "interconnected", the Act has expanded the scope of this key term to include every single computer connected to the Internet. The term "related" would have restricted the application of the term to Intranets. The author submits that such an expansive definition is wholly unnecessary and is likely to create more complications and conundrums than would have resulted from a more simplified and discrete definition such as those that had been previously proposed.

(a) Future-Proof Definitions or Definition-Proof Futures?

Within the definition of a "computer system", the term "computer" is deliberately left undefined, following the example set by the Computer Misuse Act 1990 (UK). That Act left the term undefined so as to avoid the difficulties that would be caused by future developments in technology. Even today, the term "computer" is extremely generic and subject to almost daily advances in the field of information and communication technology. Thus, the Computer Misuse Act 1990 (UK) leaves the term to be interpreted by the courts according to its ordinary usage. In direct contrast is Singapore's e-crime legislation, the Computer Misuse Act 1993 (SG), which provides a very long definition of "computer" that is not specific to a particular technology. It even extends to contemporary advances in the area of biochemical computing in an attempt to future-proof the definition:[49]

48 Crimes Bill 1989, cl 199.
49 Section 2(1) (as amended by the Computer Misuse (Amendment) Act 1998 (SG)).

> "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 —
> (a) an automated typewriter or typesetter;
> (b) a portable hand held calculator;
> (c) a similar device which is non-programmable or which does not contain any data storage facility;

The justification for the inclusion of this definition is that the widespread use of microchips, microprocessors and other similar hardware is such that a "computer" could conceivably extend to include cellular telephones, gaming consoles, and even sophisticated toasters![50]

The Computer Misuse Act 1993 (SG), in section 2(1), also defines the term "data", as "representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer". The term is undefined in most other jurisdictions, probably because the ordinary meaning of the word "data" is sufficient, and also to avoid any difficulties that could be caused by developments in technology. Despite being amended in 1998,[51] the Singaporean legislation, including the definition of "computer", continues to attract criticism for being clumsy, ambiguous, and altogether unclear.[52]

(b) The New Zealand Approach

The New Zealand statute has tried to combine the two approaches by defining "computer system" but leaving "computer" undefined. In the author's opinion, this has resulted in an overly broad and complicated definition that is wholly superfluous. The term "computer" is best left undefined – as shown by the successful application of this approach in the United Kingdom over the last 13 years, despite the radical changes in technology over this time. Indeed, any definition of computer devised in 1990 would arguably be redundant and outdated by now.

Rather, authorization and access should be delineated by varying levels – from an overall network right down to individual files and folders. Thus, the focus is shifted from computers to the data on them – what the legislation is actually intended to protect and what was originally proposed by the Law Commission.[53] By doing this, concerns and confusion about whether unauthorized access to

50 See eg "Product Directory", *Cuisinart* <http://www.cuisinart.com/cgi-bin/index.cgi/en/ item.cgi?item_id=CPT-65> (at 11 July 2004).
51 Computer Misuse (Amendment) Act 1998 (SG).
52 See eg Carr and Williams "A step too far in controlling computers?" (2000) 8(1) Int'l JL & IT 48.
53 See New Zealand Law Commission, supra note 29, 28-29.

part of a computer or network is covered (particularly in the context of guarding against insider attacks by disgruntled employees)[54] are eliminated.

2. Section 249 – Caught in a Computer System or a Cookie Jar?

This section covers access to a computer system gained for a dishonest purpose. The main elements of this section are that access must have been obtained, and that the individual who accessed it must have had a dishonest intent at the time access was obtained. The legislative purpose is to target those persons who stand to profit from hacking, or whose actions will cause another to suffer loss – in both cases, as the result of dishonesty or deception.

Two examples serve to illustrate why such a section is necessary. First, the recent case of Adrian Lamo, a hacker who allegedly accessed the Intranet of the *New York Times*, setting up five fictitious user identification names and passwords under the *New York Times*' account with *LexisNexis*, conducting more than 3,000 searches and incurring charges totalling approximately US$300,000.[55] Secondly, the earlier case of a man in Kazakhstan who manipulated software belonging to Bloomberg LP to gain unauthorized access to various customer and employee accounts in their computer system. He then sent founder Michael Bloomberg an email, attaching to it screen shots taken from within the company computer system in order to demonstrate his ability to gain access as any user. He also demanded US$200,000 from Bloomberg threatening: "There a lot (sic) of clever but mean heads in the world who will use their chance to destroy your system to the detriment of your worldwide reputation."[56]

However, subsection 249(1) does not require dishonesty, or lack of authorization to be an element in the actual *gaining* of access, only in the acts committed once access has been obtained:

> **249. Accessing computer system for dishonest purpose**
> (1) Every one is liable to imprisonment for a term not exceeding 7 years who, directly or indirectly, accesses any computer system, and thereby, dishonestly or by deception, and without claim of right,- —
> (a) obtains any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or
> (b) causes loss to any other person.

54 See Harvey, supra note 7, 193.

55 US Department of Justice "US Charges Hacker with Illegally Accessing New York Times Computer Network", Media Release, September 9 2003 <http://www.cybercrime.gov/ lamoCharge.htm> (at 11 July 2004). See also <http://news.findlaw.com/hdocs/docs/cyberlaw/ uslamo803cmp.pdf> (at 11 July 2004).

56 US department of Justice "Kazakhstan Hacker Sentenced to Four Years Prison for Breaking into Bloomberg Systems and Attempting Extortion" (Media Release, July 1 2003) <http://www.cybercrime.gov/zezevSent.htm> (at 11 July 2004). See also Stacy Albin "Bloomberg Extortionist Sentenced" *New York Times* (New York, USA, 2 July 2003) B4 (late edition, final).

The term "dishonestly" is defined earlier in the Act at section 217:

> **dishonestly**, in relation to an act or omission, means done or omitted without a belief that there was express or implied consent to, or authority for, the act or omission from a person entitled to give such consent or authority.

By implication, this allows for the prosecution of persons who misuse their authorized access with the intent of achieving financial gain or causing loss. Therefore, those people who are excluded from liability under section 252 (see below) can be prosecuted under section 249. For example, a disgruntled employee who seeks to exact revenge upon her employer by deleting or corrupting files on her employer's computer system – but only those files that the employee is authorized to access – would be liable under this subsection for at least the simple loss of the files. If the employee's actions resulted in a foreseeable financial loss to the employer, then the employee might well be liable for that too. In determining whether a person has authority or consent, it is likely that a court would ask whether the specific acts in question were authorized or consented to, not merely whether the person had authorization or consent to access the system.

Subsection 249(2) covers those who are not authorized to access a computer system but do so as a result of dishonesty or deception. The case of the Kazakhstan hacker fits this description well.[57] Noting the definition of "access" in section 248, it would seem that the term is intended to describe a continuous action. A person is "accessing" a computer system throughout the entire time that he is interacting with it. Thus, access does not just mean *gaining access* but covers the entire course of events in question, although the actus reus requirement is satisfied from the initial moment of access, possibly even from the first *attempt* at access. A physical world analogy can be made to the offence of burglary, where the actus reus is satisfied as soon as a burglar gains entry to the premises being burgled and the offence remains ongoing until she leaves. The rationale underlying this interpretation is to ensure the requisite coincidence of actus reus and mens rea – the latter in this case being a dishonest intent. Absent such an interpretation, a person who accessed a computer system without a dishonest purpose in mind, but who later formed a dishonest purpose, could not be prosecuted under this section. While it is true that he could still be prosecuted for wilful damage, and other offences related to their actions once inside the system, he could not be prosecuted for the actual act of obtaining access unless they were not authorized to access the system.

57 Ibid.

(a) Targeting Trojans

Another intended purpose of section 249 is to target those who use Trojan Horse programs to access computer systems: they may be caught under either subsection 249(1) or subsection 249(2), or both. A Trojan Horse program is one in which malicious or harmful code is contained inside apparently harmless programming or data (such as a supposed anti-virus program) in such a way that the victim is duped into installing it and thus unknowingly allowing access to their system (hence the name). A Trojan Horse that infiltrates a business system has the potential to cause financially crippling consequences. Trade secrets, confidential information, passwords, financial data, and other, sensitive information could be stolen from systems without the business's knowledge.

The focus of subsection 249(2) is on the initial access to the system, rather than on the consequent acts committed (e.g. theft). This is presumably intended as a preventative measure given that pre-existing,[58] and newly created,[59] offences already criminalize many dishonest acts that would be committed after access was obtained.

(b) Cookies and Consent

One remaining area of concern regarding section 249 is the issue of cookies. A cookie is information that a web site puts on a user's system so that it can 'remember' something about that user later. Typically, cookies record a user's preferences at a particular site. Theoretically, users must agree to accept cookies, but the "accept cookies" option is commonly set to a default "yes" by most Internet browser programs.

Given this, a problem arises in the context of section 249 – whenever a cookie is placed, the hard drive (as part of the overall computer system) is being accessed. Information communicated via the cookie benefits the owner of the web site that placed the cookie: it allows him or her to tailor that web site's services to the individual user. While the Law Commission report did not address the issue of cookies, it was the subject of an article by Dugan and Dugan in 2001.[60]

Discussing the operation of cookies in the context of what was then the Crimes Amendment Bill (No 6) 1999, Dugan and Dugan contend that "[t]he broadly worded offences [in the new Act] threaten to criminalize a range of completely innocuous activities essential to the successful operation of the Internet".[61] They point out that a machine is incapable of giving informed consent, making questions of "authority" for the receipt of cookies nebulous.

58 For example, theft under s 219 Crimes Act 1961. The definition of theft has been changed by the Crimes Amendment Act 2003 to include intangibles.

59 For example "Taking, obtaining, or copying trade secrets" under s 230 Crimes Act 1961 (as inserted by the Crimes Amendment Act 2003).

60 Dugan and Dugan, "Cookies and Electronic Crime" [2001] NZLJ 439.

61 Ibid.

There is difficulty involved in identifying any meaningful authority, "except as a matter of speculation and presumption".[62] Dugan and Dugan also point out the potential criminal implications for such activity under section 251 (making, selling, or distributing or possessing software for committing a crime) given the issues raised in relation to section 249.[63]

Consent, in the context of criminal law, means "a consent freely and voluntarily given by a person in a position to form a rational judgment".[64] While that definition is derived from a case involving consent to sexual intercourse, it nevertheless provides useful guidance in determining issues of consent in an e-crime context. Additionally, the High Court of Australia has held that a computer cannot give consent,[65] and, while New Zealand courts have yet to address the issue, it would be extremely unlikely that they would reach a different conclusion.

The law should protect Internet users from unauthorized access to their systems, but this protection should not come at the expense of criminalizing one of the most essential elements of e-commerce – cookies. However, given the potentially devastating effects of "cookie poisoning" – that is, the modification of a cookie to gain unauthorized information – as well as the issues of consent raised above, it seems that something more than caveat emptor is required for software consumers. Expecting users to read software terms and conditions before installation is one thing, ensuring their comprehension is another. Currently, only the most knowledgeable of users would be aware that they are sending cookie information along with their uniform resource locator ("URL") request. Furthermore, the issue of criminal liability may arise as new versions of existing products are released into the market, with the aim of becoming more streamlined and user-friendly. Dugan and Dugan give the example of an Internet browser that automatically accepts all cookies, without providing configuration tools to alter this setting and without informing the user about the absence of cookie policies. They suggest that such a browser may leave software developers liable to criminal prosecution.

Given the lack of technical knowledge possessed by most users, it could also be argued that, because of the strong likelihood of misunderstanding on the part of the user, all but the most detailed cookie notifications would fall afoul of section 249. While a user may be prompted to decide whether to accept or reject a cookie, there is typically no explanation of what this means. The user is not informed about why the cookie is being sent, or what the information in the cookie represents. Indeed, most users do not even have a general understanding about the operation, benefits and risks of cookies. Thus, it is evident that the cookies issue has been given insufficient thought, and needs urgent attention to amend and clarify the vagueness in the existing law.

---

62 Ibid 440-441.
63 Ibid 441.
64 See *R v Brewer* 1994 2 NZLR 229 (HC), (26 May 1994) unreported, Court of Appeal, CA516/93, 7.
65 *Kennison v Daire* (1986) 160 CLR 129.

3. Section 250 – Electronic Inoculation?

Section 250 directly targets damage and impairment resulting from hacking and other related activities. It is divided into two subsections, based on the seriousness of, and threat posed by, the illicit activities contemplated. Each subsection attracts correspondingly different penalties.

(a) Weapons of Mass Destruction: Subsection 250(1)

Subsection 250(1) addresses attacks on computer systems causing damage or disablement where "danger to life is likely to result". It is intended to deter attacks against "vital" facilities such as ports, hospitals, airports, power stations, and communications facilities by imposing a severe sanction (up to ten years' imprisonment) on those convicted of committing such offences. The requisite mens rea of the offence is knowledge that the intentional or reckless destruction, alteration or damage of the computer system will result, or is likely to result, in danger to life.[66]

An example of the type of actions that the offence is intended to cover is the recent case in the United Kingdom of a hacker who allegedly conducted an electronic attack against a major seaport in the United States. This 2003 incident that is "thought to be the first time that part of a country's national infrastructure has been disabled by an electronic attack".[67] However, it is difficult to say whether such an attack would constitute an offence under subsection 250(1), given that the subsection requires damage to, or destruction of the computer system in question. No doubt in cases such as this, where the application of the Act is unclear, prosecutors will simply stretch the wording to fit – as they did to prosecute hacking before the Act was passed. Indeed, stretches of logic may not even be required, given that the data on a computer system is altered every time that the system is accessed.

Another case from the United States is perhaps more relevant to the New Zealand provision. It involved a juvenile hacker who disabled a key telephone company computer that serviced the local airport.[68] "As a result of a series of commands sent from the hacker's personal computer, vital services to the Federal Aviation Administration control tower were disabled for six hours in March of 1997."[69]

66 Harvey, supra note 7, 188.

67 "US port 'hit by UK hacker'", BBC News, 6 October 2003 <http://news.bbc.co.uk/2/hi/ 3168696.stm> (at 11 July 2004). The defendant was later acquitted at trial. See "Teenager cleared of hacking" BBC News, 17 October 2003 <http://news.bbc.co.uk/2/hi/3197446.stm> (at 11 July 2004).

68 US Department of Justice, "Juvenile computer hacker cuts off FAA tower at regional airport", Media Release, 18 March 1998, <http://www.cybercrime.gov/juvenilepld.htm> (at 11 July 2004).

69 Ibid.

(b) Denial of Service: Subsection 250(2)

Subsection 250(2) comprises three paragraphs. Paragraphs 250(2)(a) and 250(2)(b) are similar to subsection 250(1), with three notable differences. First, there is no requirement that "danger to life is likely to result" from the acts covered. Secondly, they are more specific than subsection 250(1) in stating the elements that need to be proved in order to establish the relevant offence. Thirdly, the actus reus component is considerably broader than subsection 250(1): instead of using the subsection 250(1) formula "destroys, damages, or alters", paragraphs 250(2)(a) and 250(2)(b) cover anyone who "damages, deletes, modifies, or otherwise interferes with or impairs any data or software in any computer system", or causes this to happen. Given the fact that the data in a computer system is modified every time that system is accessed, the scope of these two paragraphs is overly broad, raising the very real possibility of excessive criminalization.

Paragraph 250(2)(c) is more specifically directed towards the criminalization of denial of service attacks. "Denial of service" is undefined in the Act, but a useful definition can be found on the *searchSecurity website*:[70]

> [A denial of service is] the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services. In the worst cases, for example, a Web site accessed by millions of people can occasionally be forced to temporarily cease operation. A denial of service attack can also destroy programming and files in a computer system.

Interestingly, the *searchSecurity website* also includes viruses and attacks on physical infrastructure within the definition of this term. Although the latter would be more easily covered by the offence of wilful damage, the former is certainly an important (although unintended) inclusion: the Act does not specifically cover the transmission of viruses.[72]

Virus use or transmission could also be prosecuted under subsection 250(1). This is illustrated by an incident in which the US Department of State's electronic system (used for checking every visa applicant for terrorist or criminal history) failed worldwide because of a computer virus, leaving the United States Government unable to issue visas.[73] Given today's heightened security concerns, the potential for danger to life is apparent. Furthermore, subsection 250(1) does not require the offender to have gained access to the system affected, thus

70 "Denial of Service: a searchSecurity Definition", searchSecurity.com, <http://searchsecurity. techtarget.com/sDefinition/0,,sid14_gci213591,00.html> (at 11 July 2004).

71 Ibid.

72 Although the possession, sale or supply of a virus would be covered under s 251.

73 "Virus knocks out State Department's visa-checking system", MercuryNews.com, 23 September 2003, <http://www.siliconvalley.com/mld/siliconvalley/6844499.htm> (at 11 July 2004).

allowing for prosecution of remotely committed offences such as the transmission of a virus or logic bomb,[74] as well as denial of service attacks.[75]

4. Section 251 – Innocent but Deadly?

Section 251 addresses the making, selling, distributing, or possessing of software for committing a crime under the new Act. Obviously, the section is intended to target so-called hacking programs, and also viruses. Supposed hacking programs, such as "Back Orifice", allow a 'master' to control and monitor 'slave' computers running the Windows operating system. Viruses, such as the "Blaster" and "Melissa" viruses, have recently caused considerable damage, in both physical and economic terms, worldwide. Indeed, the more recent "Blaster" virus also provides an example of a prosecution for an offence somewhat similar to that created by this section. Jeffrey Lee Parson was charged with "knowingly [developing] and [releasing] onto the Internet the B variant of the Blaster computer worm being an offence under US Federal law", the relevant law catching "[whoever] knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer".[76]

However, the offence under the United States Code focuses on transmission, while the corresponding New Zealand offence focuses on the distribution of software as a commodity. Of course that is not to say that a similar prosecution would not be possible under subsection 251(2):[77]

> (2) Every one is liable to imprisonment for a term not exceeding 2 years who —
>
> (a) has in his or her possession any software or other information that would enable him or her to access a computer system without authorisation; and
>
> (b) intends to use that software or other information to commit a crime.

74 "Code surreptitiously inserted into an application or operating system that causes it to perform some destructive or security-compromising activity when specified conditions are met". "Logic Bomb", The Free Dictionary, <http://www.computing-dictionary.thefreedictionary.com/logic%20bomb> (at 13 August 2004).

75 An attack which "aims to prevent legitimate users from accessing computer services". "Denial-of-Service Attack", The Free Dictionary, <http://encyclopedia.thefreedictionary.com/ Denial+of+service+attack> (at 13 August 2004).

76 18 USCS 1030(a)(5)(A)(i); United States Department of Justice, "Minneapolis, Minnesota 18 year old Arrested for Developing and Releasing B Variant of Blaster Computer Worm", Media Release 29 August 2003 <http://www.cybercrime.gov/parsonArrest.htm> (at 11 July 2004); Criminal complaint, "US v Parson", <http://news.findlaw.com/hdocs/docs/ cyberlaw/usparson82803cmp.pdf> (at 11 July 2004).

77 Parson used the "Blaster" virus to gain remote access to, and control over, a number of computer systems, then used them to conduct a distributed denial of service attack on the Microsoft Windows Update site.

The difficulty raised by section 251 is knowing precisely what "software or other information" would enable a person to gain access to a computer system without authorization.[78] It is likely that "other information" is intended to refer to passwords, security keys, and other means of bypassing security systems, but the question of what kind of software will fall under section 251 remains.

Under subsection 251(1), the software must "enable another person to access a computer system without authorisation", and must have the commission of a crime as its sole or principal use. The term "sole or principal use" is problematic. Much software can have dual use capability – even something as notorious as "Back Orifice" can easily be used for innocent as well as devious purposes. Furthermore, commonly available password-recovery programs are an obvious magnet for hackers, yet these programs too have clear legitimate uses.[79] Therefore, the phrase "sole or principal use" does little to help determine when software is likely to run afoul of this section.

Some guidance can be obtained from paragraph 251(1)(b), which creates an alternative offence, being the promotion of such "software or other information" as "being useful for the commission of a crime ... knowing or being reckless as to whether it will be used for the commission of a crime". Therefore, the factor determining whether or not software falls within the scope of this section may be how it is promoted. If this is correct, then the section is essentially futile in its objective – all a person would have to do is promote a potentially illicit program as being for a legitimate purpose, leaving the rest up to the imagination of the user.

Alternatively, the section may lead to excessive criminalization of software, meaning that any software which has the potential for misuse in the hands of the unscrupulous would be targeted. Software such as "PCAnywhere" is, on its face, legitimate software that allows users remote access to their personal computers.[80] However, the fact is that there is very little difference between "PCAnywhere" and "Back Orifice", other than the way in which the general public perceives them:[81]

> The real difference between BO2K [Back Orifice 2000] and other remote control software is its presence. Software such as PCAnywhere leaves footprints all over the OS to let you know it's installed and running. BO2K, on the other hand, leaves little if any finger prints on the system.

Even then, as one story from *CNN.com* reveals, sometimes the line between legitimate and illicit can become blurred to the point of invisibility. A user of the

78 Earwater and Heron, "NZLS Seminar, Crimes Amendment Act 2003" (New Zealand Law Society, Wellington, 2003) 16.

79 See Password Recovery Software, <http://www.lostpassword.com> (at 11 July 2004).

80 See "Symantec, Inc pcAnywhere" *Symantec* <http://www.symantec.com/pcanywhere/ Consumer/index.html> (at 11 July 2004).

81 Rob Zorn, "The Infamous Back Orifice", Actrix News, January 2000 <http://editor.actrix.co.nz/ 0001.htm> (at 11 July 2004).

"PCAnywhere" software suddenly found himself able to access another, unrelated user's system, thus becoming a hacker unintentionally.[82] Furthermore, Cult of the Dead Cow, the makers and distributors of the "Back Orifice" software, have asserted that it is a legitimate remote administration tool similar to "PCAnywhere" and other similar software products:[83]

> Built upon the phenomenal success of *Back Orifice* released in August 98, BO2K puts network administrators solidly back in control. ... BO2K is a lot like other other major file-synchronization and remote control packages that are on the market as commercial products. Except that BO2K is smaller, faster, *free*, and *very, very extensible.* ... BO2K is an obvious choice for the *productive* network administrator.

The developers of the "Back Orifice" software have answered the obvious question "Is this a 'hacker tool', or is it an 'administration tool'?":[84]

> This tool, like other tools ... can be used legitimately, or it can be used to harm people. You can take a hammer and beat people in the head with it. ... Imagine a *whole world* of people that don't know a hammer from sponge, let alone what a hammer is good for, and you'll find what situation we're in here. Hackers can use it to hack. Administrators can use it to make their lives a lot easier. Administrators, be responsible with this tool. End-users, don't trust random people on the internet, and they won't hit you with a hammer ....

Thus, "Back Orifice" should be considered no more or less illicit than "PCAnywhere". Depending on how broadly the statute is interpreted, both programs are either legitimate remote administration tools, or illicit implements for hacking. The very nature of such software is that it allows a person to obtain access to computer systems without authorization. Therefore, given the fact that legitimate and illegitimate software of this type are essentially indistinguishable, the best approach, in the author's view, would be for investigators and prosecutors to bypass subsection 251(1) altogether in favour of section 252, which deals with the consequences of illicit software use. Returning to the example of the "Back Orifice" software, the question of its legitimacy or lack thereof is a moot point. As long as it can clearly be used for legitimate purposes, and is not promoted as being useful for illegitimate purposes, it will not breach section 251. Many common tools can be used to cause harm, but possession or distribution of them is not criminalized, because context and intent are two key factors in determining criminality.

Paragraph 251(1)(b) does have a specific mens rea component (an individual must know, or be reckless as to whether the software will be used for the

82 Mark Gibbs, "Opinion: Difficult to become a hacker? It's easier than you think" *CNN.com*, February 12, 1999, <http://www.cnn.com/TECH/computing/9902/12/hack.idg/> (at 11 July 2004).

83 "BO2K – What is BO2K" <http://www.bo2k.com/whatis.html> (at 11 July 2004). Emphasis in the original.

84 "BO2K General FAQ", *SourceForge.net:* <http://sourceforge.net/docman/display_doc.php?docid=12704&group_id=4487#question_3> (at 11 July 2004). Emphasis in the original.

commission of a crime). However, this is not particularly helpful. The line between legitimate and illicit is blurred at the best of times, and often practically invisible. Parliament may have assumed that knowledge or recklessness can be implied from the nature of the software but this is clearly not the case. The provision is, in reality, tainted by a considerable degree of uncertainty and consequently is either practically useless or potentially dangerous.

5. Section 252 – Pure Hacking: not Just Fun and War Games[85]

Section 252 criminalizes "pure hacking", that is the simple act of accessing of a computer system without authorization.[86] Pure hacking can be equated to the physical world offence of trespass – the criminality lies in the act of entry itself, regardless of whether or not any damage or harm results. However, given that pure hackers do not have a malicious intent and, in some cases, arguably perform a public service by highlighting security deficiencies, there is some debate over whether or not this activity should be criminalized. The argument in favour of criminalization is based on the fact that, regardless of whether damage results, victims of pure hacking will inevitably suffer financially as a result of the intrusion. Victims will have to reconfigure their security systems to prevent repeat intrusions, and it may not be immediately apparent that the hacker did not cause any damage. Nicholl summarizes the pure hacking problem:[87]

> Many believe that criminalising benign [or "pure"] hacking trivialises the criminal law. The contrary view is that one's computer is the on-line equivalent of private property and it should be protected from unauthorised entry as is one's home or land. The New Zealand [law] favours the latter view. In most cases access will be intentional because it is not often that the steps necessary to gain access can be performed accidentally .... Proving intention to gain access is unlikely to cause problems. Far more complex is the question whether authorisation exists. This is because authorisation in the context of this [section] is subjective .... Authorisation in this context ... will [often] have to be inferred from all the circumstances.

The question of authorization is likely to be the key issue in any investigation or prosecution under section 252. Others have also raised questions about how far the term "access" extends, and when it is likely to be considered "unauthorized". This question is especially pertinent, given the broad definition of "computer system" in section 246.

---

85 DeMarco, "It's Not Just Fun and 'War Games' – Juveniles and Computer Crime", *US Attorneys' Bulletin* May 2001.

86 For a discussion of pure or "ethical hacking" see Palmer, "Ethical Hacking" (2001) 40(3) IBM Systems Journal 769.

87 Nicholl, "Computer Misuse" [2002] NZLJ 84, 85.

(a) The Ambit of Unlawful Access

In the United States, a computer science student discovered that MediaMax copy-prevention software on compact discs could be bypassed by simply holding down the shift key, or by using basic system configuration tools to disable a driver installed on the disc.[88] After the student published his findings, the producer of the software threatened to sue him under the anti-circumvention provisions in the Digital Millennium Copyright Act 1998 (US) (these threats were later withdrawn).[89] Based on the terms of this section, and on the definition of "computer system" – which extends to cover, inter alia, "all related storage [and] software facilities" including compact discs – those same actions (that is, holding down the "shift" key or disabling the driver) would constitute a crime, while using more rudimentary methods to achieve the same result (such as drawing on the compact disc with a marker pen) would not.[90]

Bruce Simpson raises another example of potential difficulties. He asks whether intentionally accessing the unsecured file directory of a web site would constitute an offence under this section:[91]

> [U]nder the terms of the [Crimes Amendment Bill], the mere act of typing in a 12-digit [Internet Protocol] number as described above, or just clicking the wrong link to someone's poorly configured webserver, could leave me liable to prosecution as a "hacker" ... Is this "breaking and entering?" In the case of the [Crimes Amendment Bill] a case could probably be mounted that it is. In the "real world" – entering someone's house without permission (even if they leave their door open) and taking something is a crime that is easy to detect ... In cyberspace however, an evil villain can rifle through all your files and download copies without the owner even being aware they have a problem.

The vagueness of section 252 is clearly a cause for concern. While the subjective mens rea requirement would protect those who inadvertently stumble across file directory listings, those who view them intentionally (say, after following a link from another site or returning after an initial, inadvertent visit) could well be prosecuted for hacking. Ironically, those who point others in the direction of such listings could escape prosecution provided their initial visit is unintentional and unrepeated.

---

88 Halderman, *Analysis of the MediaMax CD3 Copy-Prevention System*, Princeton University Computer Science Technical Report TR-679-03, October 6 2003 <http://www.cs.princeton.edu/ ~jhalderm/cd3/> (at 11 July 2004).

89 §1201 Digital Millennium Copyright Act 1998 (US). See also "Shift-Key Case Rouses DMCA Foes" *Wired News*,11 October 2003 <http://www.wired.com/news/digiwood/0,1412,60780,00. html> (at 11 July 2004).

90 "CD Crack: Magic Marker Indeed" *Wired News* (20 May 2002) <http://www.wired.com/news/ technology/0,1 282,52665,00.html> (at 11 July 2004).

91 Bruce Simpson, "Click – Oops, You're in Trouble" *Daily Aardvark*, 28 February 2003 <http://www.aardvark. co.nz/daily/2003/0228.shtml> (at 11 July 2004).

(b) Advancing a Rational Approach

In the author's opinion, the most simple and rational solution to the problem of whether or not access is authorized is to examine it in context. If a file directory, for example, were not protected, then an honest but mistaken belief of authorization would provide the person concerned with a prima facie defence. In relation to Intranets, this approach is even simpler, given that every user has a designated level of access — if the user exceeds this, then they will be acting without authorization. Nevertheless, the MediaMax situation shows that a number of circumstances are rendered problematic by the effects of section 252, as well as by the overall effect of the Act itself.

Under subsection 252(2), a person is exempted from prosecution under subsection 252(1), where "[that person] accesses a computer system for a purpose other than the one for which that person was given access". In relation to this point, Judge Harvey (writing extra-judicially) has raised the problem of "a disgruntled employee who deletes the computer hard drive containing the company's most confidential information would escape liability if he or she has authority to access the computer system".[92] While it is true that businesses are more vulnerable to insider attacks, committed by those who have the requisite level of authorization and ability to gain access, this problem is not confined to computer systems. Indeed, it is analogous to an employee shredding a large number of confidential paper documents, which she has access to, and is authorized to be in possession of but obviously not to shred. The New South Wales Court of Criminal Appeal has addressed the issue:[93]

> [T]he "authority" referred to [in the s 76C Crimes Act 1914 (Cth)] is authority to destroy, erase, alter or insert the particular data; and general authority to gain access to or use the computer is not sufficient if the particular entry etc is not authorised.

In reaching that conclusion, the Court drew an analogy with a trespass case, where it was held that "a person whose entry to premises is authorized for a particular purpose enters as a trespasser if he enters for any other purpose".[94] The Supreme Court of Victoria made a similar finding:[95]

> Where, as is the case here, the question is whether the entry was with permission, it will be important to identify the entry and to determine whether that entry was within the scope of the permission that had been given .... In the case of an employee the question will be whether that employee had authority to affect the entry with which he stands charged. If he has a general and unlimited permission to enter the system then no offence is proved. If however there are limits upon the permission given to

92 Harvey, supra note 7, 193.
93 *Gilmour v Director of Public Prosecutions (Cth)* (1995) 43 NSWLR 243, 247.
94 Ibid. See *Barker v The Queen* (1983) 153 CLR 338 (HCA).
95 *Director of Public Prosecutions v Murdoch* [1993] 1 VR 406, 409-410.

> him to enter that system, it will be necessary to ask was the entry within the scope of that permission? If it was, then no offence was committed; if it was not, then he has entered the system without lawful authority to do so.

Therefore, a strong rationale underlies the exception provided under subsection 253(2). It protects employees from criminal liability for what essentially amounts to mere tortious negligence (leaving employers to seek damages through civil proceedings), while also protecting employers from acts committed with malicious intent, ultimately reaching what the author considers to be a healthy compromise between competing interests.

III: Future Directions: The Invisible Man Defence

One issue that has achieved media prominence is that of defences to e-crime charges. One publicized case involved an attack on a Houston port facility by a hacker based in the United Kingdom. The jury acquitted the defendant, accepting his contention that unidentified vandals installed an 'attack script' on his computer, via a Trojan Horse, which he inadvertently activated. Forensic analysis of his computer revealed no trace of this program, leading the defendant to argue that it must have self-destructed.[96] This case presents a very real and pressing concern for authorities – as acknowledged by a number of security experts.[97] As one put it: "The ... case suggests that even if no evidence of a computer break in is unearthed they might still be able to successfully claim that they were not responsible for what their computer does, or what is found on its hard drive."[98] Problems arising as a result of this obvious chink in the e-crime armour are equally relevant in New Zealand. However, identification of a problem is one thing, resolving it may not be as easy. This case undoubtedly has implications for how e-crime cases are prosecuted. An expert witness who gave evidence for the prosecution stated the difficulty:[99]

> It's very difficult to counter the quite simple argument that someone else did it and ran away. We had hoped to show that if someone else did it they would have left footprints and that, in this case, there weren't any. It's difficult to prove something hasn't happened.

Interestingly, this case was the first under the Computer Misuse Act 1990 (UK) to be decided by a jury, leading to suggestions from both sides that more

96 "Teen computer whiz cleared in Houston hacking" *The Associated Press*, 17 October 2003 <http://www.securityfocus.com/news/7242> (at 11 July 2004).

97 See "Questions cloud cyber crime cases" BBC News, London, United Kingdom, 17 October 2003 <http://news.bbc.co.uk/2/hi/3202116.stm> (at 11 July 2004).

98 "Teen hacker cleared by jury" *Sophos*, 17 October 2003 <http://www.sophos.com/virusinfo/ articles/caffrey.html> (at 11 July 2004).

99 "Caffrey acquittal a setback for cybercrime prosecutions" *The Register*, London, United Kingdom, 17 October 2003 <http://www.theregister.co.uk/content/55/33460.html> (at 11 July 2004).

complex cases such as this might better be tried before a panel of experts, rather than a jury.[100] The ultimate issue is one of credibility and strength of argument. Therefore, the onus rests with the prosecutors. Prosecutors must first advance a solid case – particularly with regard to forensic evidence, one of the weaknesses in this case[101] – and secondly present that case in a way that enables both jurors and judges to understand the evidence and issues presented, without being dazzled by the technology involved. This will in turn, require prosecutors to ensure to that they understand the issues (rather than relying on experts) and present them in a clear, concise and comprehensible way.

IV: Conclusion – Toy Makers And Playmakers

The Crimes Amendment Act 2003 "addresses significant gaps that have been highlighted by the courts ... and should make the [principal Act] more practicable to use in today's ... environment".[102] It is, as one investigator aptly put it, the "new toy in the box" for investigators and legal professionals alike.[103] However, questions remain as to whether those who have been given this new toy actually know how to play with it. It is true that a successful prosecution against hackers can be brought under the pre-existing laws.[104] However, the new e-crime offences not only provide for a greater clarity in the law, they also allow prosecutors to present more rational arguments, with jurors and judges alike no longer being required to stretch their imaginations to comprehend them.

Nevertheless, there is a tendency to view issues such as those raised in this article as being the concern of a small sector of the community and not warranting general concern. Even those who do claim to have some understanding often have shallow knowledge, leading to misunderstandings caused by assumptions that can, in turn, be passed onto others as a result of over-confident claims of expertise. This is true of individuals involved in all aspects of the law – from lawmakers, to lawyers, to investigators. Given the broad-brush approach taken by the legislation, the chance that this lack of understanding will lead to error is extremely high.

The boundaries of the Act are broad as evidenced by the definition of "computer system", which extends to include all peripherals and storage media. While the Act could not be described as a 'knee-jerk' reaction – given its lengthy legislative history – it is nonetheless a somewhat clumsy tool, which may be potentially damaging when wielded by those lacking a sufficient level of

100 Ibid.

101 See "Expert witness dismisses UK hacking suspect's defence" *Silicon.com* (9 October 2003) <http://silicon.com/news/500022/1/6345.html> (at 11 July 2004).

102 New Zealand Police, *A Guide to the Crimes Act 1961 as amended by the Crimes Amendment Act 2003* (Wellington, July 2003) 1.

103 Anthony Trenwith, Interview with Duncan Gardiner, E-crime Analyst, New Zealand Police (Auckland, 23 September 2003).

104 See discussion in Part I above.

understanding. Uncertainty and disparity will inevitably result if case law is left to focus the wide boundaries established by the Act. Parliament would be well-advised to assist in this regard by 'tweaking' the legislation to provide for greater clarity, in line with the issues raised in this article.

The law is considered to be "always speaking",[105] even if what it is saying is not entirely clear. The purpose of the Act was to provide for greater clarity in the law, by (inter alia) creating specific sections criminalizing contemporary offences. While some sections are well drafted, and their intended targets clear, the same cannot be said for all sections. Parliament has seemingly found itself drawn in different directions – between discrete, directed offences on the one hand, and general, broad-based offences on the other – and, unable to decide, has attempted to go both ways. The definition of "computer system" alone is ample evidence of this dichotomy of desire.

Without clear direction, the responsibility for resolving the issues discussed in this article, and others, will fall to the courts, who, along with most counsel, are less able to avail themselves of expertise than Parliament and thus more susceptible to error. Certainly some of these errors will favour otherwise 'guilty' defendants, and others will likely prejudice the innocent. Public opinion of the quality of the legislation will be the real victim in both cases. The new Act undoubtedly has the potential to make a substantial impact in its intended area, but for that potential to be realized, the relevant provisions need to be further refined to give greater direction and certainty to the law, and to avoid hard cases making bad law.

105 See *R v Misic* [2001] 3 NZLR 1, 8 (CA), citing *Birmingham City Council v Oakley* [2001] 1 AC 617 (HL) per Lord Hoffman, citing *R v Ireland, R v Burton* [1998] AC 147, 158-159 per Lord Steyn.