DEBUGGING COMPUTER CRIME

A 13-Year Analysis of the

"Crimes Involving Computers"

Provisions of the Crimes Act 1961.

Amy Jessica Corkery

A dissertation submitted in partial fulfilment of the degree of
Bachelor of Laws with Honours

University of Otago, Dunedin, New Zealand
October 2016

ajc_1_nz@hotmail.com

Acknowledgments

To my supervisor, Associate Professor Margaret Briggs,
a constant source of wisdom and inspiration
and a champion of the ‘minimalist’ approach;

To my parents, Frances and John,
for their years of love and support;

To my friends, my flatmates, and my fellow residents of 9N12,
who have made this year so special;

To Sean Mackay, proof-reader extraordinaire;

And finally, to Waiana Mulligan, Nikky Fraser, and Jarred Griffiths,
for always being there to keep me sane and smiling.

Table of Contents

"You know, you can do this just as easily online."

Image source: Peter Vey, "You know, you can do this just as easily online": originally published in *The New Yorker* 16 January 2006 <http://www.art.co.uk/products/p15063409832-sa-i6846580/peter-c-vey-you-know-you-can-do-this-just-as-easily-online-new-yorker-cartoon.htm>

Introduction

The term "debug" came into popular usage in 1947, when a computer system at MIT[1] started malfunctioning. Admiral Grace Hopper discovered the source of the trouble: a moth – a real-world bug – had flown into the room-sized computer, and become stuck on an electrical switch.[2]

Today, debugging is an important stage in the development of computer programs. It involves finding flaws in computer programs ("bugs", though no longer of the moth variety), and designing solutions for correcting them. At the end, a report is produced, structured as "[t]his is what we have, this is what we should have instead, so fix it."[3]

This work aims to debug the computer crime provisions of ss 248-252 of the Crimes Act 1961 in a legal sense: firstly, to understand their intended function; secondly, to report how their actual function differs from this; and, thirdly, to recommend strategies for fixing the bugs. Each of these aims corresponds with a Chapter in this work.

In Chapter I, the central question will be how we want the 'program' of our statute to function. The legislative background of these sections will be examined, as well as the wider policy context that surrounds them. This will start at first principles: namely, what it means to refer to a 'computer', a 'computer system', and a 'computer crime', and how these concepts fit into ss 248-252.

'Computer crime' can include wrongful acts that affect computer systems, and wrongful acts that are effected using computer systems. It will be strongly contended that the purpose of ss 248-252 should be limited, where possible, to the first type of act.

Computer systems provide various functions, such as faster communication and efficient access to data, to such an extent that this functionality constitutes a *sui generis* public good. The central contention of this work is that the purpose of ss 248-252 is to protect these 'amenity interests'. The legislative scheme, and judicial interpretation of it, should comport with this purpose.

In Chapter II, against this backdrop, the question will then turn to how the program of our statute is set up to function in practice, and how it diverges from achieving this 'protection of amenity interests' purpose.

---

[1] The Massachusetts Institute of Technology.

[2] Boris Veldhuijzen van Zanten "The very first recorded computer bug" (19 September 2013) TheNextWeb <http://thenextweb.com/shareables/2013/09/18/the-very-first-computer-bug/>

[3] Yegor Bugayenko "Five Principles of Bug Tracking" (24 November 2014) <http://www.yegor256.com/2014/11/24/principles-of-bug-tracking.html>

This will constitute an intensive examination of the statute law in New Zealand regarding computer crime, incorporating an assessment of judicial interpretation of ss 248-252 and comparison with equivalent provisions in other jurisdictions. Sections 248 and 250-252 all need some adjustments, the majority of them minor ‘tweaks’, in order to fix bugs that have been observed or might arise. However, s 249 is more troubling because it specifically penalises the use of a computer system to commit a crime: this is inconsistent with the idea that computer crime law should only protect amenity interests, and it has resulted in a concerning body of case law.

Finally, Chapter III will be a ‘bug report’, recommending ‘bug fixes’ that have been identified in Chapter II. It will also describe new offences, and new elements of current offences, that would make the sections more congruent with the intended function of computer crime law, criminal law, and the law in general.

Chapter I: Background, Purpose, and Principles

I Background

Before examining the bugs, it first is vital to understand the program in question: why it was written, and the function it was designed for. In a legal context, this will involve examining the concept of computer crime, the history of New Zealand's computer crime law against an international backdrop, and the context and effects of computer crime.

A "Computer System" and "Computer Crime"

All of New Zealand's "computer crime" law involves acts affecting a "computer system" – illegitimately accessing it, damaging it, and so forth. Therefore, it is important to firstly understand what a computer system is, and then how one might act criminally in regard to it.

Computer systems have been around since the early 19th century, and digital computer systems began to emerge around the early 20th century.[4] Exploitation of them has occurred as long as they have existed: the ways that they can be exploited are as numerous as the functions that they can perform.

The concept of a 'computer' or 'computer system' can mean many different things.[5] Many would think of a 'computer system' as being something sitting on an office desk. On its physical component of "hardware", it will employ logical methods ("programs" or "software"[6]) to control and process information that is stored as "data".[7]

However, the forms a computer system can take can go far beyond this typical conception. They can occur across thousands of computers (a "network"), and on objects one might not think of as being computers: for example, the computer system on a calculator, or the computer system embedded within a microwave.[8]

The functionality a computer system can provide is infinite: the more functionality that a computer system provides, the more hardware, software and data will be involved. The social networking website "Facebook", for example, is not a single computer system: it is a grouping

[4] For more, see Paul Ceruzzi *A History of Modern Computing* (2nd ed., MIT Press, Massachusetts, 2003) at 1

[5] Merriam-Webster defines it as "a programmable, usually electronic, device that can store, retrieve, and process data": "Definition of 'computer'" Merriam-Webster Dictionary Online <http://www.merriam-webster.com/dictionary/computer>

[6] These logical methods have various names, depending on what they are meant to do. Others are "routines", "packages", "procedures", "algorithms", or "functions".

[7] For more, see generally Tony Bradley *Essential Computer Security: Everyone's Guide to Email, Internet, and Wireless Security* (Syngress, Massachusetts, 2006)

[8] This is reflected in its definition in the Act in s 248, where the definition of "computer system" includes "interconnected computers", "communication links between computers", and combinations of the two: Crimes Act 1961, s 248 definition of computer system, (a)(ii)-(iv). This is discussed further in Chapter II.

of many different computer systems that perform tasks such as checking the correctness of a password entered, allowing a user to upload a picture, and maintaining the storage of user data.

Disruption of this function can occur by poor design, by accident – or purposefully, as the result of the commission of a computer crime. Computer crime is mainly concerned with the exploitation of software and data, because these are the key components that give the computer system this functionality. Hardware, then, is relegated to being a 'venue' for this interaction. Because it is the physical part of the computer system (i.e. can be seen and touched), it attracts separate protection from property law.

The form of this disruption can vary. It can constitute the gain of large amounts of personal information, using complex software and affecting millions of computers:[9] conversely, it can be as simple as gaining a password by looking over another person's shoulder as they type.[10]

In New Zealand, the Crimes Act 1961 ("the Act") recognises certain forms of computer crime. Its four heads of liability are ss 249-252, and a fifth section (s 248) defines key terms for them.

Section 249 criminalises accessing a computer and subsequently doing something else wrongful. An example of this would be attacks with "ransomware," which enters a computer system and 'locks' its files and programs until a ransom is paid.[11] Section 249 could be violated where a defendant attacks other computer systems using ransomware, for the dishonest purpose of making a financial gain.

Section 250 criminalises damaging a computer system, in the sense of interfering with the data on it, or disrupting its ability to function properly. For example, in August 2016, the Australian Government Census website was rendered unusable.[12] The website's computer systems were overloaded with 'too much to do',[13] which impaired its function, and so would likely constitute damage under s 250.

---

[9] See, for example, Timothy Lee "The Sony hack: how it happened, who is responsible, and what we've learned" (17 December 2014) Vox <http://www.vox.com/2014/12/14/7387945/sony-hack-explained>

[10] *R v Gold and Schifreen* [1988] 1 AC 1063 (HL) is a case featuring this. There, the defendants looked over the shoulder of a British Telecom engineer who was in the process of inputting their password – which was "1234".

[11] New Zealand has the second-highest rate of ransomware attacks in the Southern Hemisphere. For more, see Morgan Tait "NZ in sophisticated cyber crime attack" (April 12 2016) New Zealand Herald Online <http://nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11621227>

[12] "Census: Australian Bureau of Statistics says website attacked by overseas hackers" (10 August 2016) ABC News <http://www.abc.net.au/news/2016-08-10/australian-bureau-of-statistics-says-census-website-hacked/7712216>

[13] 'Denial-of-service' (DoS, or DDoS) attacks are a common way to do this. See above n 7 at 257: "A Denial-Of-Service attack floods a network with an overwhelming amount of traffic, thereby slowing its response time for legitimate traffic or grinding it to a halt completely."

Section 251 criminalises possession of, and trading in, materials that might be used to commit a computer crime.[14] In 2011, Sony had 77 million users' credentials stolen from its PlayStation Network's computer systems:[15] s 251 would penalise possession of these credentials.

Section 252 criminalises accessing a computer system without authorisation: for example, the process by which "hackers" (individuals who use "their knowledge of networks and computer systems to gain unauthorised access to computer systems"[16]) released the email of the United States Democratic National Committee in August 2016. This was done by an 'unauthorised access' of the computer systems storing their email.[17]

All of these sections, as well as s 248, will be closely discussed in Chapter II.

[14] See above n 7 at 42 and 140. The general term for such programs is "malware" (malicious software).
[15] Ben Quinn and Charles Arthur "PlayStation Network hackers access data of 77 million users" (26 April 2011) The Guardian <https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data>
[16] Above n 7 at 258
[17] Lily Newman "Security News This Week: The DNC Hack Was Worse Than We Thought" (13 August 2016) Wired.com <https://www.wired.com/2016/08/security-news-week-dnc-hack-worse-thought/>

B Responses

This section considers the history of New Zealand's response to computer crime, and the international community's response more generally.

1 Policy responses

Criminal sanctions must be one part of a broad policy approach, because computer crime can be very difficult to prevent, investigate, and prosecute.[18] The following graphic illustrates their role.

Figure 3.7: Substantive focus of cybercrime instruments

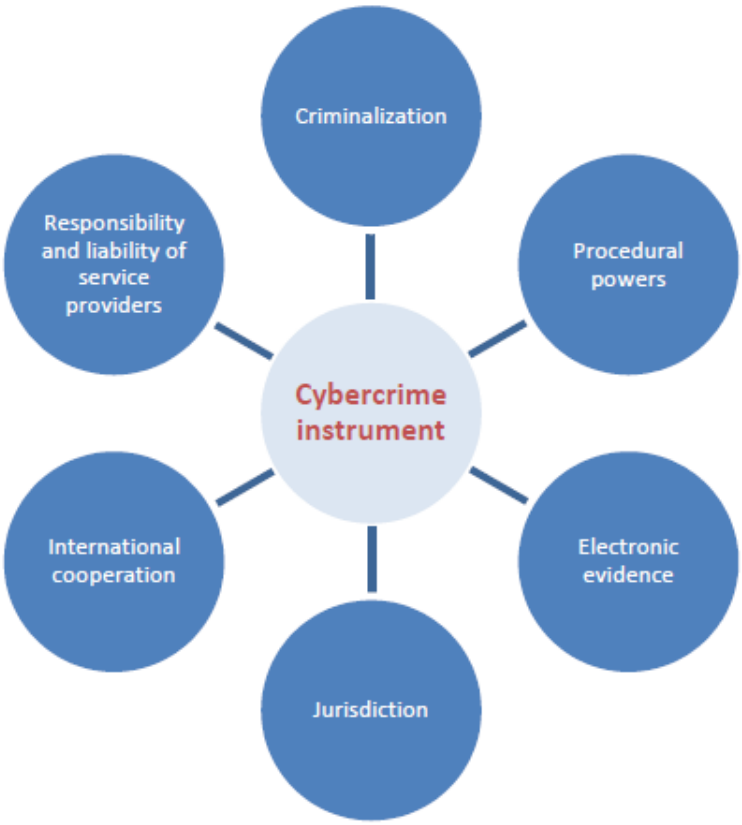

Image source: United Nations Office on Drugs and Crime *Comprehensive Study on Cybercrime: Draft* (Vienna, 2013) "Figure 3.7: Substantive focus of cybercrime instruments" at 68

[18] For more, see generally Anthony Reyes, Richard Brittson, Kevin O'Shea, and James Steele *Cyber Crime Investigations* (Syngress, Massachusetts, 2007)

The level of difficulty in responding to computer crime has caused some commentators to put the efficacy of criminalisation into question.[19] However, this work will proceed on the assumption that the need for a robust policy to respond to computer crime does not negate the requirement for criminalisation.

Policy-makers also need to prioritise international standardisation of legislation, the setting of clearer rules on jurisdiction, the granting of investigative powers, and the formation of a framework for forensic evidence.[20] All of these are important considerations, but beyond the scope of this work.

Many countries – including New Zealand,[21] the United States,[22] the United Kingdom,[23] Canada,[24] and Australia[25] – have implemented, or are in the process of implementing, their own 'cyber-security strategies' that constitute at least part of this broader policy approach.

Part of New Zealand's 'cyber-security strategy', released in 2015, is as follows:[26]

> *Elements of New Zealand's legislative framework will be tested to see whether amendment to effectively prevent, investigate and respond to cybercrime is required. This would be a targeted review.*

Chapter II of this work will focus on possible amendments to the Act to effectively prevent, investigate and respond to cybercrime.

New Zealand has a modest body of case law that examines ss 248-252, and few of these cases involve examples of what people would consider the archetypal 'computer criminals'.[27] However, this is not indicative of the level of computer crime it experiences: a report from April of this year found that it is subject to 108 computer crimes per day.[28]

The number of cases will only increase: it is therefore vital that our legislation is examined, so bugs are detected and fixed early. A robust and 'future-proof' legislative structure is also vital

---

[19] See generally Gregor Allan "Responding to Cybercrime: A Delicate Blend of the Orthodox and the Alternative" (2005) 2 NZ L Rev 149, and Lawrence Lessig "The Law of the Horse: What Cyberlaw Might Teach" (1999) 113 Harv L Rev 501

[20] United Nations Office on Drugs and Crime *Comprehensive Study on Cybercrime: Draft* (Vienna, 2013) at xi

[21] Department of the Prime Minister and Cabinet *National Plan to Address Cybercrime 2015* (December 2015) <https://www.connectsmart.govt.nz/assets/Uploads/nz-cyber-security-cybercrime-plan-december-2015.pdf>

[22] Executive Office of the President of the United States, "The Comprehensive National Cybersecurity Initiative" WhiteHouse.gov (Washington D.C., 2008) <https://www.whitehouse.gov/sites/default/files/cybersecurity.pdf>

[23] Cabinet Office of the United Kingdom *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world* (London, 2011)

[24] Royal Canadian Mounted Police *Royal Canadian Mounted Police Cybercrime Strategy* (Ottawa, 2015)

[25] Department of Prime Minster and Cabinet *Australia's Cyber Security Strategy: Enabling innovation, growth & prosperity* (Canberra, 2016)

[26] Above n 21 at 11

[27] This will be discussed below in the introduction to Chapter II, at page 34.

[28] Above n 11

for reasons of international uniformity and for the congruous workings of New Zealand's criminal law.

2 Legal responses

(a) New Zealand law

New Zealand's computer crime laws have a protracted history. After being initially drafted in 1989, they were passed "hastily"[29] as part of a large Amendment Act. This was done partially as a reaction to a perception, sparked by the events of the time, that computer systems in New Zealand were not protected adequately by the existing law.

In 1989, the Fourth Labour Government elected to develop a Crimes Bill containing the first draft of today's provisions:[30] it was designed to achieve "an excellent criminal code that will see New Zealand through into the next century."[31] The Minister of Justice assembled a Crimes Consultative Committee to issue a report on the Bill as a whole, which they did in 1991.[32] However, the Government of the time did not prioritise the issue, and so the legislation did not proceed further.

A decade later in 1998, however, a renewed interest in the Bill was partially caused by *R v Wilkinson*.[33] While there was no 'computer crime' committed in that case, it involved an electronic transaction that the wording of the Act did not cover: this contributed to a narrative that the Act was becoming 'out-dated'. The defendant had falsified invoices to suggest he owned unencumbered assets, for the purposes of gaining a loan. The Court of Appeal held, relying in part on the English case of *R v Preddy*,[34] that the defendant had not satisfied the elements of the charge of theft because he obtained a mere "chose in action" – the ability to draw on that loan. This did not constitute a thing "capable of being stolen", which was an element of theft in the Act at the time.[35]

In addition to the problem highlighted in *R v Wilkinson*, and in the absence of specific provisions covering computer crime, computer criminals were being charged under other miscellaneous legislation. This raised questions about how far the wording of that legislation could 'stretch'. In one case, for example, it fell to the Court of Appeal to determine the question

---

[29] Scott MacLeod "Hacker tapped into accounts, police claim" (30 June 2000) Stuff.co.nz <http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=118209>
[30] Crimes Bill 1989 (152-1)
[31] Crimes Consultative Committee *Crimes Bill 1989: Report of the Crimes Consultative Committee* (April 1991) at 5
[32] Above n 31
[33] *R v Wilkinson* (1998) 16 CRNZ 179
[34] *R v Preddy, Slade and Dhillon* [1996] UKHL 13
[35] Above n 33 at 188

of whether a computer program could be a "document" for the purpose of a charge of "dishonest use of a document".[36] Such cases also came amidst growing concern about the dangers posed by hackers: in 1998, Paul Holmes interviewed "a 15-year-old boy known as Spasrat, believed to be the computer hacker who destroyed more than 4000 websites".[37]

The cumulative effect of all of this was a renewed belief that the Act needed computer-specific offences.[38] The Law Commission issued a report in May 1999 on the topic, entitled "Computer Misuse"[39] ("the Law Commission report"). The Bill containing ss 248-252 was brought to Parliament in September of that year,[40] and it came into force four years later as the Crimes Amendment Act 2003 ("the Amendment Act").[41]

(b) International law

The main international law instrument on computer crime is commonly known as the Budapest Convention.[42] New Zealand is broadly compliant with this,[43] but has not yet acceded to it.[44] This demonstrates some legislative recognition of the wider international context, though, which continues today in the judiciary. In *Cai v R*, Miller J opined:[45]

> *Although New Zealand has yet to adopt the [Budapest] Convention, the legislative history suggests that s 249 should be interpreted in a way which aims to preserve the integrity of electronic banking systems.*

[36] *R v Misiç* [2001] 3 NZLR 1 at [38]
[37] Interview with 'Spasrat' (identity obscured), computer hacker (Paul Holmes, "Holmes", 20 November 1998)6. TVNZ archive record at <https://1drv.ms/b/s!AlUY72FCRVHGzwduXvEfw0GqCF3V>
[38] See, for example, the second reading of the Amendment Act ((5 October 1999) 580 NZPD 19732): the Hon. Phil Goff stated that "we have had recent cases where people have done enormously expensive damage through hacking, and action has not been able to be taken against them. Last year a hacker destroyed 4,500 web pages hosted by The Internet Group..."
[39] Law Commission *Computer Misuse* (NZLC R54, 1999)
[40] (7 Sept 1999) 580 NZPD xv. The First Reading is not in Hansard, but was nevertheless recorded in its Index as happening on that day.
[41] Crimes Amendment Act 2003
[42] Council of Europe Convention on Cybercrime (opened for signature 23 November 2001, entered into force 1 July 2004)
[43] This was also the view of the Select Committee that considered the Amendment Act: Crimes Amendment Bill (No 6) 1999 (322-2) and Supplementary Order Paper No. 85 (select committee report) at 19
[44] Part of New Zealand's cyber-security action plan is that it "consider" doing so, however: above n 21 at 14.
[45] *Cai v R* [2011] NZCA 604 at [20]

II Purpose and Scope of Regulation

Before debugging the provisions, their wider context must be examined. This entails understanding why the concept of technology-neutral legislation is essential in this context, the reasoning behind the separate regulation of computer systems, and why property law cannot provide adequate protection for this.

A Categories of Computer Crime

The Budapest Convention,[46] and some organisations in other jurisdictions,[47] conceive of computer crime in four general 'groupings'.

The first of these is where crimes are committed against a computer system ('computer-system-as-target'). This type of offence conceptualises the computer system as the thing that needs protecting in and of itself – the information stored on it remaining private, for example, and access to it being restricted to those with permission. The second is crimes committed using a computer system ('computer-system-as-tool'): for example, using a computer to steal trade secrets.[48]

The third is crimes involving storage on a computer system (for example, a collection of digital spreadsheets that indicate a money-laundering scheme, or the storage of scanned images of child pornography). Issues related to computer systems in that context will be more closely related to evidence law: for example, the validity of search warrants granting access to them. Similarly, the fourth part – which covers the criminal dimension of copyright infringement – is most relevant to the law of intellectual property.

1 'Computer-System-as-Tool' Offences

An essential distinction in this work is the one between 'computer-system-as-target' offending (the undermining, degrading, or diminishing of the proper function of computer systems) and 'computer-system-as-tool' offending (general wrongful behaviour, of any type, with the involvement of a computer system).

---

[46] Above n 42. Title 1 of the Convention (Arts. 2-6) is called "Offences against the confidentiality, integrity and availability of computer data and systems"; Title 2 (Arts. 7-8) is called "Computer-related offences"; Title 3 (Art. 9) is called "Content-related offences"; Title 4 (Art. 10) is called "Offences related to infringements of copyright and related rights".

[47] The Canadian police refer to "technology-as-target" and "technology-as-instrument" offences in their computer crime strategy document (above n 24 at 7). So too does the United States Department of Justice in prosecutorial guidelines on the subject (see H. Marshall Jarrett, Michael Bailie, Ed Hagen, and Scott Eltringham *Prosecuting Computer Crimes* (2nd ed., United States Department of Justice, Washington D.C., 2010) at v)

[48] Criminalised by s 230 of the Crimes Act 1961.

There are many acts that could constitute 'computer-system-as-tool' offences. This is because computer systems offer many amenities, so there are myriad wrongful acts that can be committed using them – theft, for example. There can also be civil actionability: perhaps in tort, for using computer systems to defame someone;[49] or intellectual property, for directly copying the 'source code' of a computer program.[50] Computer data can be protected by causes of action such as company,[51] privacy,[52] equity,[53] and contract[54] law.

The question then arises as to when wrongful behaviour with a computer system should come within the scope of computer crime law. If a bank employee looked up a customer's confidential file where she had no legitimate reason to, actions might arise in privacy law, contract law, and employment law. When would it be appropriate for a cause of action to arise in computer crime law – possibly for unauthorised access under s 252? Would the employee have to hack into a co-worker's computer – or would the unauthorised conduct of looking up the file be enough? These issues will be discussed further in Chapter II.[55]

B Purpose: 'Computer-System-as-Target' Offences and their Protection of Amenity Interests

The central contention of this work is that the wording and scope of ss 248-252 should be the protection of computer systems from 'computer-system-as-target' offending. This is the function of the 'program' of New Zealand's computer crime law. The scope of ss 248-252 should not extend into the realm of penalising general wrongful conduct that involves the use of a computer system.

---

[49] See, for example, *Murray v Wishart* [2014] NZCA 461 at [170]: there, the comments alleged to be defamatory were posted on the social media websites Facebook and Twitter.

[50] See, for example, the copyright action for a computer program in *Fisher & Paykel Financial Services v Karum Group* [2012] NZHC 3314 at [85]

[51] See, for example, the New Zealand Institute of Directors' report on such issues (New Zealand Institute of Directors *Cyber-Risk Practice Guide* (New Zealand Institute of Directors, Wellington, 2016))

[52] For more, see Bruce Slane, Privacy Commissioner "Privacy protection: A Key to Electronic Commerce" (New Zealand Law Conference, Rotorua, 9 April 1999)) <https://privacy.org.nz/news-and-publications/speeches-and-presentations/privacy-protection-a-key-to-electronic-commerce/ >

[53] See, for example, the equitable breach of confidence action in *Force India Formula One Team Limited v Aerolab SRL & Anor* [2013] EWCA civ 780. Force India's confidential company designs, stored on a computer system, were disclosed to another Aerolab client without permission.

[54] An example of this might be an alternative version of the *Force India* action (above n 53), if the action was for a breach of a contract. For example, one of its terms could being the secrecy of any of Force India's intellectual property.

[55] See the below heading "Removal of the exception in s 252(2)?", on page 37. For the purposes of this example, the possible effect of s 252(2) has been ignored.

1 "Technology-Neutral" Legislation

One of the central goals of criminal law is to preserve personal autonomy while maintaining the welfare of society in general.[56] In a computer crime context, this means that the criminal law should adopt a 'hands-off' approach where behaviour is not 'criminal in nature',[57] especially where civil-law actions might also apply.

Thus, even though computer crime is a serious societal problem, it does not necessitate the intervention of the criminal law wherever there is wrongful conduct that involves a computer system. The application of computer crime law should be more narrowly focused on the computer system as the thing in need of protection.

However, this is one of two competing conceptions of what computer crime law 'should be'. It is a "technology-neutral" approach, as opposed to one of "technology-exceptionalism".[58] Where law is technology-neutral, 'technology-based' offending is not treated as being inherently different to 'real-world' equivalents without good reason. However, where there is general wrongful behaviour that uses a computer ('computer-system-as-tool' offending), and it is punished with a computer crime offence, it can make serious inroads into that concept.

A technology-neutral approach is the better 'default,' to be departed from where the inherent characteristics of computer systems differ from 'the real world' in that the paradigm of the offending is genuinely different or the prospect of harm is inherently higher. If the prospective harm is treated as inherently higher without firm justification, that is undesirable technology-exceptionalism. It conceptualises computers as being inherently dangerous, whereas a technology-neutral approach better recognises that they are simply *de rigueur* in modern life.

Over time, computer systems will be used more to commit many varieties of wrongful behaviour. It will become increasingly counterintuitive to take this approach and penalise the use of a ubiquitous tool. This is especially so in the case of offences such as s 249 – which specifically penalise the use of a computer to commit an offence that is already subject to legislative sanction. For example, if an accountant stole from her employer using a computer-based accounting system, she would be liable both for the theft and for the use of a computer system to commit it.[59]

In this context, a technology-neutral approach will encompass the ideas that statutory maximum sentences should be the same as their 'real-world' equivalents; that offences that

---

[56] See generally Andrew Ashworth and Jeremy Horder *Principles of Criminal Law* (7th ed., Oxford University Press, Oxford, 2013), chapter 2

[57] The question of when behaviour is 'criminal in nature' is discussed at page 20, under the heading "Why provide this protection?".

[58] For more on the history and background of 'technology-exceptionalism', see Eric Goldman "The Third Wave of Internet Exceptionalism" (11 March 2009) Technology & Marketing Law Blog <http://blog.ericgoldman.org/archives/2009/03/the_third_wave.htm>

[59] This occurred in *Police v Knight* DC QUN CRI-2011-059-001363, 16 January 2012.

might be committed using technology are defined using terminology that can encompass that method of commission; and, centrally to this work, that wrongdoing is not penalised more heavily (or with more available charges) purely by virtue of use of technology in its commission.

Linguistic ambiguity will always mean that 'computer-system-as-target' offending could theoretically 'spread too far' and capture 'computer-system-as-tool' offending as well. However, this can and should be minimised. There is a possibility of this occurring in all of ss 248-252, but the most notable subversion of the technology-neutral concept is s 249: this specifically penalises the use of wrongful behaviour using a computer system.

There is strong support of the concept of technology-neutral law from the legislature.[60] There is also judicial approval of it, such as that from the Court of Appeal in *R v Mark Hayes* (*Hayes* hereafter):[61]

> *[T]he approach to sentencing for computer based crime should start by reference to penalties that would have been imposed had the crime been committed through paper based means.*

2 Support for the proposition

The legislative history of the Bill shows a subtle but definitive shift in the conception of the purpose of computer crime. In 1989, when the provisions were initially drafted, computers were conceived more as something to be 'dealt with' and protected from. The Rt Hon Geoffrey Palmer MP referred to what is now s 249 as being for the "dishonest use of a computer whether access is lawful or not."[62]

However, a decade later, the Law Commission report specifically recommended that all forms of access be 'unauthorised' to be considered criminal:[63] the 1989 Bill only required that a computer be used.[64] Technology-neutral legislation was considered a valuable goal by Members of Parliament during the passage of the 1999 Bill,[65] and by the Law Commission in reports such as *Computer Misuse*[66] and *Electronic Commerce*.[67] Many amendments have also been made to the Act to make 'traditional' offences applicable to a technology context. The

---

[60] Discussed further below under the heading "Support for the proposition", at page 19.
[61] *R v Mark Hayes* CA CA197/06, 24 November 2006 at [77]
[62] (2 May 1989) 497 NZPD 10425
[63] Above n 39 at 4 and 88
[64] Above n 31 at 75: "Clause 200: Accessing computer, etc., for dishonest purpose"
[65] At the second reading of the Bill ((5 October 1999) 580 NZPD 19732) the Minister of Justice stated that "It is vital that we make our legislation technology-neutral and describe the nature and the form of the offence rather than the specifics of the mechanism by which it was done." Similarly, at 19736, Dr Wayne Mapp MP also referenced "the whole issue of technology-neutral legislation and harmonisation."
[66] Above n 39 at 6
[67] Law Commission *Electronic Commerce Chapter One* (NZLC R50, 1998) at 114

definition of the word "document", for example, formerly involved "material used for writing or printing",[68] whereas the current definition is much wider: "material by means of which information is supplied".[69]

This is also supported by the scheme of the statute. It has provided separate sections that specifically apply to computer systems, while following the same structure as their 'real-world' equivalents. An example of such a pair is "Damaging or interfering with computer system"[70] and "Intentional damage".[71]

The computer misuse offences were also passed at least partially in response to several high-profile hacking incidents;[72] the proposition that other forms of law were not sufficient to address this form of offending;[73] and the idea that computer systems were vital "infrastructure".[74]

In international law, the Budapest Convention references other forms of 'computer–system-as-tool' offending, but without any indication that such offending should be treated more seriously. This provides support at international law for the proposition that the law be technology-neutral unless there is good reason to make it otherwise.

3 Why provide this protection?

The purpose of the provisions should be to protect computer systems from 'computer-system-as-target' acts. It is worth noting that this protection is criminal in nature, and the reasons for this must be examined.

The first thing to note is that such 'computer-system-as-target' offences are not technology-neutral. The postal service forms a part of New Zealand's infrastructure, but Parliament has not provided legislative protection for the methods the postal service uses to transport mail between cities. Why are computer systems worthy of their own protection?

[68] This (in full, "any paper, parchment, or other material used for writing or printing, marked with matter capable of being read"), appeared in the Crimes Act 1908 s 288, and was replaced by the Crimes Amendment Act 1973 s 5.
[69] Crimes Act 1961, s 217
[70] Crimes Act 1961, s 250
[71] Crimes Act 1961, s 269
[72] For more, see above heading "New Zealand law" at page 14.
[73] For more, see below heading "Examples of the approach" at page 22.
[74] See, for example, the Consideration of the Report of the Select Committee: ((17 June 2003) 609 NZPD 6324), per Hon Tony Ryall MP: "when it comes to supporting the infrastructure to ensure that we have security and that the rights of the owners of computer infrastructure are protected, this Government is sadly wanting."

The answer must be that it is because they provide us with the ability to perform 'real world tasks' at a much higher speed and scale. This 'heightened level of ability' constitutes a paradigmatic shift, such that the regulation of computer systems is *sui generis*.

Computer systems are ubiquitous in modern society: they are common in everything from air traffic to automatic lighting systems. They are also becoming increasingly connected to one another, and to the Internet:[75] entire economies depend on them.[76] They provide society with functions like communication, information and content delivery, productivity enhancement, and the ability to operate across borders. This makes them a public good that is worthy of protection by the criminal law. Additionally, if they cannot be trusted to perform these functions, their potential utility cannot be fully realised.[77]

In a very general sense, behaviour is 'criminal in nature' where there is serious wrong against an individual, or a fundamental societal value or institution. In this case, the wrong is of such a 'degree' that it rightly concerns the state and not just the individual affected.[78] Civil or regulatory liability can also arise, but the type of wrong committed is greater than that which those remedies were designed to address.[79]

Computer crime law does not exist for the protection of computer systems as separate legal 'persons', or as a 'precious dominion' that is not to be encroached upon. Instead, it protects them because the sum total of their numerous functions constitutes a public good – such that interference with these systems necessitates the intervention of the state.

Criminal law scholars[80] posit four interests that are protected by criminal law: physical/bodily integrity, material support and amenity, freedom from humiliation and degrading treatment, and privacy and autonomy.[81] While the first and third of the two are not as prominent in this context, harm to the amenity provided by computer systems (and its flow-on consequences) can cause serious detriment to the second and fourth. Financial harm, as one of these flow-on consequences, is estimated to cost New Zealand businesses $250,000,000 annually.[82]

---

[75] For more discussion of this increasing connectivity, see Andy Taylor "The Internet of Things, cyber-security and the role of the CIO" (20 September 2016) SC Magazine UK <http://www.scmagazineuk.com/the-internet-of-things-cyber-security-and-the-role-of-the-cio/article/521127/>

[76] At above n 74, Parliament recognised this: per Brian Connell MP, "The importance of computer systems to the New Zealand economy is something that we cannot understate. In fact, I do not think that we can overstate it, either."

[77] Additionally, if a computer system's functionality is disrupted, it may not only have an atomic effect on that one computer: in some forms of computer crime (see, for example, "The Heartbleed Bug" (2014) Codenomicon <http://heartbleed.com/>), many computers could become vulnerable. Their increasingly interconnected nature means that malicious software can have a large-scale effect quickly.

[78] Glanville Williams "The Definition of a Crime" (1955) 1 CLP 1

[79] Andrew Ashworth *Principles of Criminal Law* (5th ed., Oxford University Press, Oxford, 2006) at 1-3

[80]]See, for example, Andrew von Hirsch and Nils Jareborg "Gauging Criminal Harms: A Living Standard Analysis" (1991) 11 Oxford J Legal Stud 1

[81] Above n 79 at 37

[82] "Cyber crime – the hidden epidemic hurting our businesses" (2 May 2016) New Zealand Herald Online <http://www.nzherald.co.nz/sponsored-stories/news/article.cfm?c_id=1503708&objectid=11630920>

Similarly, the privacy interests of users were severely diminished in the hack and release of user data of extramarital-affair website Ashley Madison.[83]

Protection of amenities is seen in the Act: in sections such as "Endangering transport"[84] and "Waste or diversion of electricity, gas, or water".[85] It is useful to understand computer systems' cumulative 'heightened level of ability' as such 'amenity interests', in three different 'groupings' described in the Budapest Convention. The first of these is computer systems' integrity – their correct and complete operation; the second is their availability – the ability for users to access them; the third is confidentiality – that they are sufficiently private and secure.[86] Additional to these is also the ability for users be assured of (and to trust in and rely upon) these attributes.

Computer crime law can protect many different aspects of these three interests. Across jurisdictions, it addresses areas like malicious impairment of their function; using them without authorisation, or causing them to deny authorised users access; 'eavesdropping' on their connections; or erasing or corrupting the data held on them.

For example, the Internet shopping website ASOS provides users with the ability to buy clothing from anywhere in the world, at any time of day, without leaving their houses (an amenity sometimes called "e-commerce"). Damage to the integrity and availability interests of its website with a denial-of-service attack (s 250) would mean that people could not access it. Furthermore, hackers accessing the website illegitimately (s 252) and stealing users' credit card information and purchase history (s 251 and s 249) would affect ASOS' confidentiality and security. This would have subsequent detrimental effects on users' privacy, and on the financial interests of both ASOS and its users. The wider effect of that attack would be that both parties would have their trust in that computer system, and possibly in computer systems generally, diminished. They might then be less likely to utilise them for future e-commerce transactions.

C 'Computer-System-as-Target' Protection with Property Law?

Hacking into a computer system without permission (now s 252), adopting a property-law-metaphor approach, could translate to criminal trespass.[87] Similarly, this might make s 249

[83] Tom Lamont "Life after the Ashley Madison affair" The Guardian (28 February 2016) <https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked>
[84] Crimes Act 1961, s 270
[85] Crimes Act 1961, s 271
[86] Above n 42, in Preamble
[87] Criminalised by Trespass Act 1980 s 10.

analogous to burglary,[88] s 250 to intentional damage,[89] and s 251 to possession of burglary tools.[90]

However, extending these provisions would not be appropriate. Property law cannot provide this protection. Certainly, before there were specific criminal sanctions regarding 'computer-system-as-target' offences, judges used this approach, but the framework is not a good fit for the computer crime context.

1 Examples of the approach

In the first iteration of the Bill in 1989, it was explicitly stated that "traditional property offences cannot deal adequately with misconduct in respect of computers";[91] similar sentiments were seen in the Law Commission report in 1999.[92]

However, before ss 248-252 were enacted, there was an argument that the law provided adequate protection of computer systems. During the passage of the Bill, a newspaper technology editorial read:[93]

> *'In New Zealand there is no law against hacking.' I've been hearing this statement since about 1985… it's a lie… Just look at how well New Zealand courts are dealing with hackers.*

An example of this approach is *R v Garrett*.[94] The defendant installed malicious software that gave them remote control over the hard drives of their victims: this allowed for the uplifting of their information and the deletion of their data. The charge was 'wilful damage' to property: the Court held that such acts could constitute criminal damage because the defendant had altered the magnetic particles on the hard drives, which impaired their operations.

However, there was recognition of the problems that the metaphorical approach created: *R v Gold & Schifreen* is an example of this in the United Kingdom.[95] The defendants accessed British Telecom's computer systems and the user data they contained (including Prince Philip's

[88] Criminalised by Crimes Act 1961 s 231.
[89] Criminalised by Crimes Act 1961 s 269.
[90] Criminalised by Summary Offences Act 1981 s 14.
[91] Above n 31 at 74
[92] Above n 39 at [75]
[93] Chris Barton "Anti-hacking policy masks hidden agenda" New Zealand Herald Online (5 March 2003) <http://www.nzherald.co.nz/technology/news/article.cfm?c_id=5&objectid=3198788>
[94] *R v Garrett* [2001] DCR 955
[95] *R v Gold & Schifreen* [1988] AC 1063, above n 10. Similarly to *Wilkinson* in New Zealand, *Gold and Schifreen* was the impetus for the passage of the United Kingdom's own computer crime offences in their relevant Act: see John Leyden "'80s hacker turned journo, IT crime ace Steve Gold logs off" (13 January 2015) The Register http://www.theregister.co.uk/2015/01/13/steve_gold_obit/>

saved ‘voicemail’ messages). The access was gained using an illegitimately-obtained password.[96]

They were charged with defrauding by manufacturing a “false instrument”,[97] that instrument being the ‘state’ of the British Telecom computer system “after it had processed Gold's eavesdropped password”. The House of Lords, dismissing the conviction on appeal, described this interpretation as follows:[98]

> *The Procrustean attempt to force these facts into the language of an Act not designed to fit them produced grave difficulties for both judge and jury which we would not wish to see repeated.*

However, despite this type of case causing judicial discomfort, the language of property has persisted after 2003: possibly because judges want to keep the definition of property ‘ambulatory,’ or because of a familiarity with property law.

In a Supreme Court decision in 2015, *Dixon v R* (*Dixon* hereafter),[99] the defendant was convicted for acquiring a digital video file from his employer’s computer. The Court considered that file to be property. Section 249, the charge in this case, lists possible things that can be obtained – “any property, privilege, service, pecuniary advantage, benefit, or valuable consideration” – to attract criminal sanction. It provides alternatives that fit the fact situation better and would not have attempted to construct a property-law metaphor to give computer data the same characteristics as a physical videotape.

“Benefit” was favoured by the Court of Appeal in that case,[100] and is more suitable. The defendant undoubtedly obtained a benefit – this being the ability to sell the footage for profit. Using that definition would have meant that the Court would not have to enter the muddled territory of re-affirming the common law concept that information is not property,[101] while holding that the data forming the computer file (either pure information, or very close to it) could be considered property.[102]

---

[96] The United Kingdom suggested another interesting approach in a discussion paper: the Theft Act 1968 (UK) s 13, “Abstraction of electricity”. This was because “the operation of a computer consumes electricity. Any unauthorised accessing of a computer would therefore seem to constitute the *actus reus* of the offence…” (United Kingdom Law Commission *Working Paper No. 110: Computer Misuse* (London, 1988) at 32). In New Zealand, this provision has never appeared in our Crimes Act, and so would not have been available. Parliament instead opted to ‘cover’ such acts by extending the definition of “property” in s 2, in the Amendment Act, to include “electricity”. (It is laid out in full below under the heading “Property law philosophy”, on page 25).

[97] Forgery and Counterfeiting Act 1981 (UK), s 1

[98] Above n 10 at [1]

[99] *Dixon v R* [2015] NZSC 147 at [23]-[24]

[100] *R v Dixon* [2014] NZCA 329 at [39]

[101] At [24]. The common law concept originated in the case of *Oxford v Moss* (1979) 68 Cr App R 183 (QB).

[102] See also: Lance Green “Does The Definition of “Property” In The Crimes Act 1961 Include Electronically Stored Data? The Computer Says “No.”” (LLB (Hons) Dissertation, University of Otago, 2015).

This case only concerned the data that the video file was comprised of: it did not involve a property law metaphor for a computer system, as such. The uncomfortable conceptual fit is, though, familiar to this context.

Assessing the charge of "access without authorisation", for example, a judge likened the offending to a "burglary", and described the access as akin to a physical trespass: "there has got to be a point of entry, either through a window or through a door or through the roof."[103] In the same vein, when blogger Cameron Slater's computer systems were hacked (again, an "access without authorisation") Fogarty J described the wrong done as "appeal[ing] to values which underpin the most ancient remedy of trespass, be it trespass to the person or trespass to property".[104]

2 Property law philosophy

The logic of approaching protection of the amenity of computer systems with property law is, at least, strained and of limited use. The comparison is useful as a 'benchmark' for technology-neutral conceptions of the seriousness of offending – the method that *Hayes* used[105] – but no further.

The Act defines property as including:[106]

> *real and personal property, and any estate or interest in any real or personal property, money, electricity, and any debt, and any thing in action, and any other right or interest.*

It is phrased in broad terms, and the inclusion of "any thing in action" would suggest any right over any thing – tangible or intangible – that could have its right to possession enforced by a legal action.[107] Any rights of property over a computer system would be an intangible "right or interest":[108] they have a physical presence in terms of their hardware, but this is a separate concept.

In his seminal work on "Ownership", Anthony Honoré identified eleven elements of property:[109]

---

[103] *New Zealand Police v Franciso Javier Correa Silva* DC WN CRI-2010-085-007353, 10 December 2010 at [22]: the case involved hacking charges under ss 251 and 252.
[104] *Slater v APN New Zealand Ltd* [2014] NZHC 2157 at [5]
[105] Above n 61 at [45]
[106] Crimes Act 1961, s 2. This definition was amended, by the Crimes Amendment Act 2003 s 4(3), to add "money" and "electricity".
[107] See Ken Moon "Intangibles as property and goods" (2009) 5 NZLJ 228
[108] Samantha Hepburn *Principles of Property Law* (Cavendish Publishing, Great Britain, 1998) at 16
[109] Anthony Honoré "Ownership" in Anthony Honoré *Making law bind: essays legal and philosophical.* (Clarendon Press, Oxford, 1961) at 165.

> *Ownership comprises the right to possess, the right to use, the right to manage, the right to the income of the thing, the right to the capital, the right to security, the rights or incidents of transmissibility and absence of term,*[110] *the duty to prevent harm, liability to execution,*[111] *and the incident of residuarity.*[112]

Hanoch Dagan outlines its features:[113]

> *Property is frequently described as a bundle of sticks: that is, a collection of substantive rights, such as the right to exclude, to use, alienate and so on… Property is frequently analyzed as a bulwark of individual freedom and independence… concerns the efficient (or inefficient) allocation of resources.*

Ziff describes how judges analyse what is encompassed by its definition:[114]

> *Two distinct styles of judicial analysis seem to exist. Some courts adopt an attributes approach… whether the right being asserted looks like property… a functional approach, by contrast, first looks at the policy factors at play.*

Ziff's first approach is to 'look for a norm' in describing the attributes of the computer system. Computer systems provide us with many valuable attributes, which fulfils Ziff's approach to property as something providing human flourishing, subjective happiness, freedom and justice, and material wealth.[115] They enable material wealth, for example, in their enabling of commerce and formation of an industry that is devoted to their creation and maintenance.

However, the comparison becomes far more tenuous when considering the vast array of forms a computer system can take. If the idea is to 'look for a norm,' their physical form occurs as patterns of electrical signals. This makes it difficult to have certainty of what the property actually comprises from second to second. Computer systems are not atomic, and good computer program design involves several interlocking parts from several sources.

This idea of property being defined mainly as a right to exclude others would fit as an idea of having a computer system that its user has the sole right to use. Blackstone's concept of a "sole

[110] i.e. that there is no set expiration date for the rights over the property.
[111] i.e. the ability to be seized as payment for debts.
[112] i.e. the ability for property rights to expire, or be abandoned.
[113] Hanoch Dagan "The Craft of Property" (2003) 91 Cal L Rev, 1517 at 1519-1520, 1558-1565
[114] Bruce Ziff *Principles of Property Law* (6th ed., Carswell, Toronto, 2014) at 53
[115] Above n 114 at 12

and despotic dominion"[116] encompasses security and privacy interests, which are an important part of the amenity provided by computer systems.

However, if computer systems are not atomic, then they are definitely not a "sole and despotic dominion", or Dagan's "bulwark of freedom and independence". The operation of computer systems involves constant interactions with other computer systems – thousands, if not millions, per second – many of which the user is not aware of and does not control.[117] In property law, the assumption is exclusion: in a computer system, however, the assumption is interaction, where only some of these interactions are worthy of criminal sanction.

It is difficult to see how this paradigm fits with many of Honoré's eleven rights, and the related metaphors quickly become laboured. Management, harm, and monetisation, for example, are all fulfilled. However, s 251 references the "possession" of software: this incorporates an element of physical control,[118] and is difficult to see how one would one 'physically control' a set of instructions that are stored in a conventional computer system as pattern of ones and zeroes.

Ziff's second approach is to look at the social value attained from applying rights of property. From an economic 'commodity' perspective, property law assists a society by helping to efficiently allocate scarce resources. Computer systems are not a scarce resource. Again, their physical component is, and perhaps some of their 'load-bearing capacity' is too (such as a website selling tickets crashing when popular events go on sale), but software and data are infinitely replicable.

It would also be counterproductive to mix computer system jurisprudence with property law jurisprudence where the paradigms are so different. Private trespass is not usually a cross-border issue, but unauthorised access frequently is. Loading a webpage takes a significantly different form than having a book posted, and so the law that governs these transactions should be different.

The temptation to view these systems as property should be resisted: computer systems are too different to property to include in the scope of its definition. They are not an exclusive, or an atomic, entity: they are something providing amenity.

---

[116] William Blackstone *Commentaries on the Law of England 1765-1769: Volume 2* (The University of Chicago Press, Chicago, 1979) at 2

[117] See Steve Miller *The Complete Idiot's Guide to the Science of Everything* (Penguin, London, 2008) at 252

[118] Above n 114 at 134-135: "Few terms of property law are as readily found in common parlance as the word possession…at its core are two components: *animus possidendi* (an intention to possess) and *factum* (physical control)."

III Method of Regulation

The question then turns to the method that computer crime law should use to provide the appropriate regulation to achieve this purpose, and how to determine the level of criminality.

The wording of criminal law offences regulating computers must be broad. However, this invites the possibility that offences might extend beyond 'computer-system-as-target' regulation and enter the domain of penalising general wrongful conduct with computer systems.

From a legislative standpoint, this should be avoided where available with precise statutory wording that adheres to the purpose of computer crime law. From a judicial standpoint, a purposive approach will be helpful in both an assessment of the criminality of the offending, and the level of that offending.

A Assessing Criminality

Suppose 'computer' was defined in s 248 as "a metal case enclosing electronic components that allows input with a mouse and keyboard, and output to a display monitor".

This definition would be narrow, and specific. Drafting criminal offences in such terms, especially as they become more 'serious' in nature, makes them transparent and predictable in their application to the people they govern.[119] However, Parliament opted to draft the statute in language that was broader than that: 'computer system', for example, is defined as being a 'computer,' but that word is not further defined.[120]

This was because adopting narrower definitions risks 'under-criminalising' the range of offences that might occur. Future technological development is an 'unknown quantity': for example, the above definition would exclude 'tablet' computers. New methods of committing offences would either 'slip through the cracks' of the wording, or force judges to 'stretch' the wording of statutes to a problematic degree (as they did before 2003). Maintaining current wording means that the statute remains flexible enough to cover developments like smart phones[121] and wearable technologies.

---

[119] Above n 56

[120] The New Zealand Law Commission also agreed: at above n 39 at 6, "we are of the view that it is best not to define the term [computer]. We intend that the term be interpreted in a wide sense so as to include any future technology of similar kind not yet in existence."

[121] It is likely that a smart phone computer system could be considered a 'computer' for the purposes of the Act, as the literal definition of a 'computer' is wide enough to incorporate the computer system on cell phones, especially modern smart phones. See Bianca Mueller "Criminal liability for mobile phone spying in NZ" (31 January 2014) LawTalk – New Zealand Law Society <https://www.lawsociety.org.nz/lawtalk/lawtalk-

The problem with this approach is that using vague language makes the law uncertain. Where narrow language can 'under-criminalise', broad language can 'over-criminalise'[122] and cause 'computer-system-as-target' offences to apply to situations beyond their intended purpose. For example, using the torch function on a cell phone during a burglary could constitute 'access of a computer system for a dishonest purpose' under s 249. The cell phone has computer componentry, it is being used to illegitimately obtain property, and "access" is defined broadly enough to include the use of the torch. The scope of the provisions should therefore be limited (where possible) to terms that protect amenity interests.

B Level of Criminality

If the purpose of computer crime is the protection of amenity interests, then the main method of determining its seriousness should be the level to which these have been harmed. Where this harm is non-existent or negligible, then no penalty (or a lower penalty) may be warranted.

1 De Minimis Offending

Statutory phrasing in broad terms can cause issues for the *de minimis* principle in criminal law, whereby criminal remedies should not penalise 'trifling' behaviour.[123] It is something to be especially wary of where actors in all parts of the legal system – judges as well as lawyers – might not recognise when behaviour is truly *de minimis*.

If it is accepted that computer systems should be regulated using 'broader' language, then this is a bug that cannot be fixed. It is built into the system, but it needs to be managed. Where the harm to the amenity interests of computer systems is negligible, prosecution should be considered inappropriate, and a discharge without conviction[124] or a low penalty may be called for.

The "accessing without authorisation" case *R v Boyack* (*Boyack* hereafter) is a good example of low-level offending which did not involve punitive sanctions:[125]

> *You reached under a grille, turned a computer monitor towards you, and accessed the police intranet home page by using the mouse… A principal objective of s 252 is to deal with computer hacking. What you*

archives/issue-834/criminal-liability-for-mobile-phone-spying-in-nz> See also the case of *United States v. Neil Scott Kramer*, 58 ALR Fed 2d 611 (2011), which considered this question.

[122] Ashworth, above n 79 at 74-77, refers to this dichotomy as "maximum certainty" vs. "social defence".

[123] Above n 79 at 32. See also Douglas Husak "De Minimis 'Defence' to Criminal Liability" in R.A. Duff and Stuart Green (ed.) *Philosophical Foundations of Criminal Law* (Oxford Scholarship Online, 2011) part II ch.15

[124] As provided for in the Sentencing Act 2002, s 106(1).

[125] *R v Boyack* [2008] HC Auckland CRI 2007-044-002515, 6 June 2008 at [6]

> *did is far removed from computer hacking, but in a technical sense this section in the Crimes Act does cover what you did.*

Woodhouse J held that a low level of criminality was appropriate. The offending was certainly *de minimis*, and more prosecutorial discretion may have been called for. The harm caused was at a level so low that it was inappropriate for the charge: perhaps he may have damaged amenity interests if he had targeted the authentication process of the computer system, accessed sensitive material, or deleted police files.

2 Harm to Amenity Interests

Contemporary criminalisation theory analyses a wrongful act's level of criminality through two philosophical 'lenses': the degree of the harmfulness of that act, and the degree of its moral wrongfulness. The question of when these are attained (so as to make the behaviour criminal), and the subsequent 'level' of that criminality, is a matter of debate. Such debate also questions which of these two 'lenses' the criminal law should prioritise addressing.[126]

Because the purpose of computer crime law is the protection of the amenity interests that computer systems provide, the central consideration of the 'seriousness' of offending should be the degree to which they are diminished. This is a harm-centred approach.

The level of this harm can, because of the nature of computer crime, vary widely. A computer crime could range from an access without authorisation (and nothing further) effected by a twelve-year-old who was experimenting with Internet security – to this access being effected by a hacker stealing millions of dollars' worth of confidential information. An offender can illegitimately transfer themselves "$1,000,000" instead of "$1,000" through a quick press of a button:[127] on the other hand, they could have the intent to cause a nuclear reactor to shut down,[128] but lack the technical skills to enter the relevant computer system and do this.

The type of harm can also vary widely. Financial and economic harm are more apparent, but so too are harm to privacy interests, and (for example) harm to efficient government operations where there is detriment of trust in institutions that hold private data.[129]

---

[126] Above n 79 at 40

[127] See *Gao v R* [2013] NZCA 173: in that case, the computer transfer was a result of a clerical error, not a computer crime, but the ease with which the transfer occurred is telling. The defendant was accidentally granted an overdraft of $10,000,000 instead of $100,000.

[128] A successful example of this is the 'Stuxnet' virus. For more, see Kim Zetter "An Unprecedented Look at Stuxnet, the World's First Digital Weapon" (3 November 2014) Wired.com <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>

[129] An example of this arose in 2012, where questionable system design on Work and Income New Zealand kiosks meant that a casual user could access all of the files on that machine (see Kate Shuttleworth "MSD shuts WINZ kiosks after lax security exposed" (15 October 2012) New Zealand Herald Online <http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10840563>).

Considerations of moral wrongfulness are not as prominent in this context, nor are they as helpful. This is because it would likely be difficult for a judge to determine what constitutes 'moral' conduct in this context. For example, there are clear social conventions that it is morally wrong to indecently interfere with human remains;[130] but there are fewer of these relating to society's relationships with computer systems, because of the 'newness' of technology. An emerging example is social etiquette (amongst youth, especially) that others' smart phones are not to be looked through without permission.[131]

[130] Criminalised by s 150 of the Crimes Act 1961.

[131] See, for example, Matt Honan "What Not to Do with Someone Else's Phone" (6 October 2011) Gizmodo <http://gizmodo.com/5810782/what-not-to-do-with-someone-elses-phone>, Nina Evangeli "Going through someone else's phone is never OK" The Tab <http://thetab.com/2016/03/07/going-someone-elses-phone-never-ok-78499>, and the Computer Ethics Institute "The Ten Commandments of Computer Ethics" (1 September 2011) CPSR <http://cpsr.org/issues/ethics/cei/>.

IV Conclusion

If the task is to debug the ‘program’, then the first step is discovering how the program should function.

Its purpose is the protection of a *sui generis* public good. As computer systems are vital to the way societies live and work, the amenity interests they provide – integrity, availability, and confidentiality – are worthy of discrete legal protection. Computer crime law should comport with this purpose, and not extend to penalising general wrongful conduct using computer systems.

Ensuring this program runs correctly should involve a purposive approach in statutory interpretation, a technology-neutral ethos, a rejection of the use of a property law framework, and assessments of ‘seriousness’ with regard to the level of damage done to the amenity interests that computer crime law protects.

Chapter II: Analysis

With the idea of how the program should function established, the next step is to identify 'where the bugs are'. In a legal context, this entails assessing the wording of the statute, and examination of how it is being utilised by Courts – both in New Zealand and internationally.

Computer crime is frequently undetected or unreported:[132] in 2011, for example, the Police "recorded 47 offences nationwide of accessing computer systems without authorisation, and 347 offences involving accessing computer systems for dishonest purposes".[133] These figures are low in light of statistics such as "8121 [computer crime] incidents, involving losses totalling $8 million" in New Zealand in 2014.[134] It highlights that criminalisation is necessary, but a strong policy focus is still required for an effective response.[135]

This also means that New Zealand's body of case law on ss 248-252 is modest. The majority of it exists in unreported decisions of the District Court:[136] this means that where cases are available, it is often as a result of an appeal. Additionally, the fact that a case is available does not entail that it will centre on a legal analysis of ss 248-252. Thus, it is difficult to garner a complete image of how the sections are being used in practice. Section 249 is the most common charge observed in the case law, which is congruent with the above Police statistics.[137]

However, there is sufficient material to be able to examine where the bugs are appearing, especially where overseas examples can be used. Overall, the statute protects amenity interests in a comprehensive way, but there are 'tweaks' that can be made to have it only penalise 'computer-system-as-target' offending. The exception to this is s 249, which is more problematically worded. The concept of assessing the 'seriousness' of the offending with reference to amenity interests has been coherently stated by the Court of Appeal: some of the maximum available penalties in statute, however, need adjustment.

---

[132] Above n 21 at 4

[133] Francesca Lee "Hacking of Facebook often easy to do" (7 April 2012) The Press Online http://www.stuff.co.nz/the-press/news/6706956/Hacking-of-Facebook-often-easy-to-do>

[134] Chloe Winter "Cyber crime continues to rise" (18 May 2015) Stuff.co.nz <http://www.stuff.co.nz/technology/digital-living/68636916/cyber-crime-continues-to-rise>

[135] For more discussion on this, see the above heading "Policy responses" at page 12.

[136] All of ss 248-252 are punishable by a term of imprisonment of two years or more. This means that they are determined a Category 3 offence by s 4(1)(k) of the Criminal Procedure Act 2011, and so (per s 4(1)(m)) the default venue for the trial will be the District Court.

[137] As a very rough indication of this: in the Westlaw New Zealand category for "Criminal law > Offences > Computers" on 28 September 2016, there were 30 cases. Only three of them did not involve a charge under s 249.

I Property Law 'Cross-Over'

The sections are to be found in Part 10 of the Act, which deals with "Rights of property". However, many offences appear in that Part that do not strictly relate to property interests, but are closely related to them: for example, "Obtaining or causing loss by deception" (which encompasses the obtaining of many non-property interests),[138] or "Counterfeiting public seals".[139] In a similar vein, many of computer systems' amenity interests are based around property – such as financial ones, in online banking. Thus, even though this is not the focus of ss 248-252, they are best left to remain in the same place.

II Assessing Criminality: ss 248-252

In a computer crime context, the criminal law should only penalise behaviour where the amenity interests of computer systems have been adversely affected. This has many facets in considering ss 248-252.

The protection of the amenity interests of computer systems must involve broad language that can encapsulate a wide range of offending. The legislative wording must be as closely-calibrated as possible to concepts of the protection of amenity interests: this is because their purpose should not be generalised to sanctions for 'wrongful conduct using a computer'. Judges should interpret these concepts with the purpose of computer crime law in mind.

[138] Crimes Act 1961, s 240(1): "(a) … any property, or any privilege, service, pecuniary advantage, benefit, or valuable consideration, …(b) … obtains credit… (c)[obtains a document] capable of being used to derive a pecuniary advantage…(d) causes loss".
[139] Crimes Act 1961, s 261

A Sections 248 and 252

Section 248 defines the key terms “access”, “authorisation”, and “computer system”, which are used in ss 249-252. Engaging closely with these terms is vital: for example, what the “computer system” is will be vital to the question of when it has been accessed, and ascertaining its ideal function to the question of when it has been ‘damaged’.

Section 252 provides criminal liability at the intersection of the three concepts – so issues with s 248 are, by implication, issues with s 252 as well. Therefore, they will be discussed together.

252 Accessing computer system without authorisation

(1) Every one is liable to imprisonment for a term not exceeding 2 years who intentionally accesses, directly or indirectly, any computer system without authorisation, knowing that he or she is not authorised to access that computer system, or being reckless as to whether or not he or she is authorised to access that computer system.

(2) To avoid doubt, subsection (1) does not apply if a person who is authorised to access a computer system accesses that computer system for a purpose other than the one for which that person was given access.

248 Interpretation

For the purposes of this section and sections 249 to 252, —

authorisation includes an authorisation conferred on a person by or under an enactment or a rule of law, or by an order of a court or judicial process

1 “Authorisation” and Exceeding Authorised Access

The definition of this term is a prime example of the need to use a purposive approach when assessing the words of the statute to determine criminality: s 248 leaves it almost entirely to the discretion of the individual judge.

Determining the fact of "authorisation" is a complex concept in computer crime.[140] It can invite questions of which computer systems someone is authorised to access and which they are not (do you need express permission to use a co-worker's computer?); whether use for a purpose that is outside the explicit scope of authorisation is still authorised (is using Facebook on a work computer authorised, even though that is not the purpose of having office Internet access?); and whether access can still be authorised even where there is a breach of an explicit term that the authorisation was granted upon (what if it is a term of your employment contract that Facebook usage during work hours is forbidden?).[141]

In an unreported District Court case, a husband guessed the Facebook password of his estranged wife, read her messages to see who she had been contacting, and changed her password.[142] A conviction was entered under s 252: because the case is unreported, the reasons why are not available. However, it makes for an interesting 'thought experiment' as to what form a purposive analysis of the statute, focusing on amenity interests, might take.

Facebook's authentication system was not undermined, and privacy law may have also applied here. However, the confidentiality interests of the computer system were undermined, and so too was the concept that the person logging into an online account is trusted to be the 'owner' of that account.

(a) Removal of the exception in s 252(2)?

The Court in *Watchorn v R* (*Watchorn* hereafter) held that "the effect of s 252(2) is to exclude access by an employee for an unauthorised purpose from the ambit of that provision."[143] This was likely inserted as a 'stop-gap' against some of the problems arising in case law in the United States[144] and Canada.[145]

The Explanatory Note for the Bill that inserted ss 248-252 explicitly states that the subsection does not protect "employees who are not authorised to access a particular part of their

---

[140] For more, see Australian Institute of Criminology "High tech crime brief no. 5" AIC (January 2005) <http://www.aic.gov.au/publications/current%20series/htcb/1-20/htcb005.html>: "Determining whether a hack is authorised or not is not straightforward and may involve detailed consideration of whether a computer owner has any data access policy, whether and how that policy is communicated to others, how accessible a computer is, and how accessible are the files, directories and other information on that computer."

[141] These categories are partially based upon Orrin Kerr's method of 'splitting up' the offences, albeit changed slightly. For his, see Orrin Kerr "Cybercrime's Scope: Interpreting 'Access' and 'Authorisation' In Computer Misuse Statutes" (2003) 78 NYULR 1596 at 1622-1624.

[142] The news report for it is at "Marlborough man charged for hacking wife's Facebook account" (21 June 2016) Marlborough Express Online <http://ssl-www.stuff.co.nz/marlborough-express/news/81277346/Marlborough-man-charged-for-hacking-wifes-Facebook-account>.

[143] *Watchorn v R* [2014] NZCA 493 at [79]

[144] The United States' statute uses two different forms of the term in various places in their Criminal Code, but 'authorisation' is not defined in either of them. See the prosecutorial guidelines published by their Department of Justice (above n 47 at 5-6).

[145] Mike Doherty "SCI 4192 Report 1: Problematic Computer Crime Law In Canada" (October 31 2013) HashBang <https://hashbang.ca/wp-content/uploads/2013/11/report1.pdf> at 13-14

employer's computer system."[146] Where employees access *other* computer systems, to which they have not been granted access (for example, access of the payroll computer system, as opposed to the computer system containing client files), the 'bar' does not operate. There is a possibility that amenity interests could be diminished in that case: Courts will need to intensely engage with the meaning of "computer system" where this question arises.

There are commentators that view this subsection as a 'loophole'[147] in the legislation. One author has noted that the inclusion of (2) "is surprising because several studies suggest that the threat of "insider hacking" is more serious than that of external intrusions."[148] However, with the purpose of computer crime law in mind, the opposite is true: it does not extend far enough. If explicit terms that access was granted upon are breached, then the bar should still operate, because the fact of authorisation was still obtained by legitimate means and so amenity interests are not diminished. The integrity of an accountant's computer system, for example, is not diminished if she uses it to apply for a job with her employer's competitor.

Such behaviour would amount to using a computer system wrongfully, but not committing a 'computer-system-as-target' offence. The extension of s 252 to such behaviour would constitute an intrusion of the criminal law into the violation of private duties. This bug is best illustrated by case law in the United States.

In *United States v O'Brien,* the defendant "was a computer consultant for a travel wholesaler" who "made unauthorised changes to the computer system" by cancelling flight reservations.[149] His access to the computer system was authorised, but the changes he made constituted a breach of his employment contract, so he was successfully charged with a criminal offence.

In a more extreme example, *United States v. Drew*, it was alleged that the defendant "exceeded authorized access" when she violated the Terms of Service of the social networking website "MySpace" by 'cyber-bullying' another user.[150] The use of the criminal law would be inappropriate in this context. Thus, a narrow and purposive approach is called for.

---

[146] Above n 43. This caused the Court some difficulty in *Watchorn*: above n 143, at footnote 33 of the case.
[147] Judge David Harvey *internet.law.nz* (4th ed., LexisNexis New Zealand, Wellington, 2014) at 319, for example, notes that "Businesses are more vulnerable to insider attacks committed by those who have the requisite level of authorisation and ability to gain access… the difference between real world activity and unlawful activity…reduces itself to the issue of identity, anonymity and secrecy of activity."
[148] Above n 19 at 160
[149] *United States v O'Brien* 435 F 3d 36 04-2447 (2006) at [1]
[150] *United States v. Drew* 259 FRD 449 CD Cal (2009). Criminal law sanctions in the context of Terms of Service are especially concerning, as they are often not even enforceable in contract law: this can be for various reasons that include a lack of consideration, or a lack of positive assent to them. For more, see Jennifer Granick, Director of Civil Liberties at the Stanford Center for Internet and Society ("Innovation or Exploitation? The Limits of Computer Trespass Law", Stanford Law School, Stanford, California, February 19, 2013) (at <https://youtu.be/F4XdxmLUfqI?t=19m57s> at 19:57)

2 "Computer System"

> 248 Interpretation
>
> […]
> *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 communication facilities, and stored data.

New Zealand defines "computer system" comprehensively, but nowhere in that definition is the word 'computer' defined. This is curious, comparatively speaking: amongst countries that do not provide a definition, the statute is usually completely silent to the entire concept.[151]

The question of exactly which computer system is being accessed is a key component of liability for all of ss 249-252, but the statute is 'buggy' in that it does not emphasise the central attributes that a computer crime might affect. Computer systems are comprised of the components in (b), but the computer system itself occurs when they interact. They can occur across the various types of hardware mentioned in (a)(ii)-(iv), but hardware is a mere 'venue' for this interaction. The amenity interests provided by computer rely far more the dual components of software and data.

Recognition of this is important for the even application of ss 249-252. A company's 'payroll' computer system could be stored on the Internet with 'cloud-based' software, on a single computer system that is only allowed to be accessed by accounting staff, or on a central 'server' computer that accounting staff access on their own computers. All should be able to constitute a "computer system" for the purposes of ss 249-252, as unauthorised access to all of them would affect similar amenity interests of integrity and confidentiality.

[151] See, for example, the United Kingdom statute – Computer Misuse Act 1990 (UK), and the Australian statute – Criminal Code Act 1995 (Cth).

There are also examples of judges defining the term with an improper focus: in *Pacific Software Technology Ltd v Perry Group Software*, Hammond J gave a very narrow definition of the concept that heavily focused on the hardware components of the computer.[152]

3 "Access"

> 248 Interpretation
>
> […]
> *access*, in relation to any computer system, means instruct, communicate with, store data in, receive data from, or otherwise make use of any of the resources of the computer system

Access of a computer system may occur by many different methods: s 248 comprehensively covers all of these. The interpretative difficulty here will not occur when assessing the fact of access, but in the process of describing the precise nature of the 'computer system' that was the subject of that access.

[152] *Pacific Software Technology Ltd v Perry Group Software* [2004] 1 NZLR 164 at [25]-[26]

B Section 249

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.

(2) Every one is liable to imprisonment for a term not exceeding 5 years who, directly or indirectly, accesses any computer system with intent, dishonestly or by deception, and without claim of right,—

(a) to obtain any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or

(b) to cause loss to any other person.

(3) In this section, *deception* has the same meaning as in section 240(2).

Actions should be criminalised, under ss 248-252, where there is harm done to the amenity interests provided by computer systems.

However, that is not the scope of s 249(1): this section instead penalises the use of a computer to make an illegitimate gain, or an attempt to do so. The same applies to the inchoate version of the offence in subsection (2): the result is that the *actus reus* of that offence penalises behaviour that is not sufficiently proximate to criminal offending.

1 'Computer-system-as-tool' Phrasing

The ideal scope of this statutory provision should be as a 'more serious version' of s 252: i.e. amenity interests were diminished through the illegitimate gaining of access, and 'to make matters worse', there was additional harm done to other interests. An example of this would be a hack of the Bangladesh Central Bank in 2016: $81,000,000 was stolen after the unauthorised

access occurred.[153] The idea here is that the 'computer-system-as-target' offence led to subsequent 'computer-system-as-tool' wrongful behaviour, which 'worsens' the offending.

However, the only thing required with regard to the computer system is access – not "accessing without authorisation" or "accessing dishonestly". This means that it extends to the point of specifically penalising 'computer-system-as-tool' offending, which is a major bug.

In *Le Roy v Police*, Dobson J claimed that "dishonestly" referred to the defendant's method of gaining access:[154]

> *[t]here is no justification, either as a matter of interpretation, or in terms of the evident policy behind the introduction of the offence created by s 249, to require the establishment of a separate requirement attributing dishonesty to the obtaining of the benefit.*

This is an excellent example of a purposive approach being followed: however, with respect, "dishonestly" clearly semantically relates to the illegitimate gain and not to the access. *Watchorn* reinforces that idea:[155]

> *the heading… is not an accurate summary of the offence created by s 249(1)... The Crown must prove that the defendant accessed a computer system and thereby dishonestly or by deception and without claim of right obtained a benefit.*

This means the section specifically penalises the conduct of using a computer system for wrongful behaviour, which constitutes a significant extension beyond the protection of amenity interests.

An example of this can be found in *Burt v Police*, where the defendant sent an email to Fonterra telling them that they should send a payment to him to which he was not entitled.[156] He was authorised to access his email system: there was no diminishing of the amenity interests of computer systems. The charge in that case was phrased as follows:[157]

> *directly accessed a computer system, namely an ihug email account in the name of Lance Burt, and thereby dishonestly and without claim of right obtained a pecuniary advantage…*

---

[153] Joanna Slater "After Bangladesh: How a massive hack shook the banking world" (12 June 2016) The Globe and Mail <http://www.theglobeandmail.com/report-on-business/international-business/cybertheft-of-bangladeshs-central-bank-threatens-global-bank-system/article30408324/>

[154] *Le Roy v Police* HC WN CRI-2008-485-38, 25 August 2008 at [12]

[155] Above n 143 at [26]. *Adams on Criminal Law* (Bruce Robertson and Jeremy Finn (ed.) *Adams on Criminal Law: 2016 Student Edition* (Thomson Reuters, Wellington, New Zealand, 2016) at 424) also makes this point.

[156] *Burt v New Zealand Police* [2012] NZHC 2551

[157] At [9].

Instead of being charged with the wrongful act that he committed (possibly, obtaining by deception[158]), the defendant was specifically charged with using a computer system to do so. If the defendant had written a letter on paper to Fonterra requesting a release of those funds instead, he would not have attracted liability under s 249. His use of a computer system opened him up to another possible head of liability, which is the antithesis of the goal of technology-neutral legislation.

The omission of 'unauthorised' is either as a result of an implicit exception to this goal, or else it was a simple oversight by Parliament in their haste to see legislation passed. The wording in this section is taken from the original suggested legislative amendments from 1989[159] which consciously embraced a specific 'computer-system-as-tool' form.[160] In 1999, however, the focus had shifted to technology-neutral legislation and the protection of infrastructure.[161] If the framing of the offence is an implicit exception to this goal, then it is not well-supported by the idea that the purpose of computer crime is the protection of amenity interests.

There is scope, however, to claim that the use of a computer 'worsens' the offence in every case, in the same way that robbery 'worsens' theft by adding a component of violence – such that a separate provision is required. This idea was described by the judge in *R v Kerr*:[162]

> *utilisation of computers for the commission of crime is an aggravating circumstances* [sic] *in itself because of the consequences of this type of offending, the ability to avoid detection and to conduct the offending by effectively hiding behind the computer…*

There is evidence to indicate that the nature of computer-based theft can be more serious, for the above reasons and because some reports state that "a successful and undetected… thief could attack an institution repeatedly, and an institution with an unsuspected vulnerability could be victimized by multiple criminals."[163] This is reinforced by the idea that much of the s 249 case law features a theft of large quantities of money.[164]

---

[158] Criminalised by the Crimes Act 1961 s 240.
[159] Above n 30 at s 305ZD
[160] Above n 64
[161] See, for example, above n 74 – as well as general discussion under the heading "Support for the proposition" on page 19.
[162] DC WN CRI-2008-032-004266, 25 May 2009 at [19]: the judge was summarising the approach of Judge David Harvey in *Police v Greig* DC Manukau CRI 2004-092-003818, 24 May 2004. See also *Police v Dick* DC ROT CRI-2009-063-007025, 1 July 2010 at [2].
[163] Office of Technology Assessment *Selected Electronic Funds Transfer Issues: Privacy, Security, and Equity* (Diane Publishing, Pennsylvania, 1982) at 49
[164] As an unscientific representative sample of s 249 cases: *Appuhamilage v Police* [2015] NZHC 2355 featured a theft of $35,000; *Ashby v Police* [2015] NZHC 1900, $24,610; *Benjamin v R* [2012] NZSC 39, $18,081; *Burt v Police* [2012] NZHC 2551, $81,000; *McLachlan v R* [2014] NZCA 462, $11,000.

However, a higher 'range' of available loss does not mean that a separate offence is required. *Singh v Serious Fraud Office*[165] and *Serious Fraud Office v Ross*[166] are examples of this: both involved 'white-collar crime' and theft of large sums of money, but the charge was entered under s 249 in the first case and s 260 ("False accounting"[167]) in the second. Due to the advent of computer-based accounting, offences such as fraud and theft from employers will be increasingly committed using a computer. It does not seem appropriate that the law does not recognise the 'normality' of computer systems in this industry.

Additionally, grand-scale theft and loss are not necessarily guaranteed consequences of computer crime. In some s 249 cases, defendants created fraudulent auctions for goods on online auction website "Trade Me":[168] they would await payment for the goods, and then not deliver them. It is difficult to see how this offending is made inherently worse by virtue of its medium.

Furthermore, this phrasing also places us 'out of step' with the relevant framing of the offence in Australia,[169] the United Kingdom,[170] Canada,[171] and the United States.[172] Their statutes include provision that access be "unauthorised" or "dishonest".

Contrasting case law illustrates this comparative distinction. In New Zealand in *Sarah v R*, the defendant was a police prosecutor who was part of an investigation into a methamphetamine supply ring. He passed on police intelligence to the criminals involved in that investigation.[173] In the United Kingdom in *DPP v Bignall*, the police constables used the Police motor vehicle registration system for their own illegitimate purposes.[174] While the defendant in New Zealand was held liable for dishonest access of a computer, the United Kingdom defendants were not convicted of a 'computer crime' because the wrongful act did not target the amenity interests of computer systems.

This has also caused issues in terms of the body of precedent of s 249. The case law under it ranges from employees stealing funds from their employers,[175] to 'archetypal' hackers,[176] to

[165] *Singh v Serious Fraud Office* HC AK CRI 2008-404-000361, 4 March 2009
[166] *Serious Fraud Office v Ross* [2014] DCR 163
[167] Crimes Act 1961 s 260
[168] See, for example, *New Zealand Police v Whitaker* [2015] NZDC 24887, or *Amanda Renee Spence and Dominic Stormy Visser v New Zealand Police* HC ROT CRI-2007-077-001151, 25 February 2009.
[169] Criminal Code Act 1995 (Cth), s 477.1
[170] Computer Misuse Act 1990 (UK), s 2
[171] Canadian Criminal Code RSC 1985 c 46 s 342.1(1)
[172] 18 USC § 1030 (a)(1)-(4)
[173] *Sarah v R* [2013] NZCA 446
[174] *DPP v Bignall* [1998] 1 Cr App R 1
[175] See *Whangapirita v Police* [2012] NZHC 308; *Fitzmaurice v New Zealand Police* [2013] NZHC 494; *Thomas v New Zealand Police* HC AK CRI 2008-404-343, 9 February 2008; *Jardine v R* [2016] NZCA 371; and *R v Marriner* DC NWP CRI-2011-043-002852, 9 December 2011 – to name only a few.
[176] See, for example, *R v Grygoruk* HC AK CRI 2006-092-12831, 23 May 2008

child pornographers,[177] to those infringing copyright.[178] There is little in common between the fact circumstances of the case law, aside from the use of a computer system and some degree of illegitimate 'obtaining'.

2 Inchoate Form of the Offence

The wording of s 249(2) creates an inchoate form of the offence in s 249(1), by criminalising access with an illegitimate intent. The scheme of this subsection follows the pattern of other sections in the Act which penalise inchoate forms of the full offence separately, such as aggravated burglary.[179]

However, this means the *actus reus* element of the offence only involves the use of a computer system. The Act's general provision for inchoate offences, s 72, would also *prima facie* apply to this subsection:[180] this would mean the possibility of a charge of an attempt to commit s 249(2).

The United Kingdom Law Commission has pointed out, regarding their version of this provision, that:[181]

> *[t]he speed with which such a theft may be carried out using a computer, and the consequent difficulty of detecting the perpetrator, require in our view a special extension of the criminal law in order to discourage such conduct…*

Commentary on Canada's Criminal Code has also used this reasoning to explain its own version.[182] This echoes a central philosophy underpinning the law of attempt: "the social importance of authorizing official intervention before harm is done".[183] Specific provision for an attempt may be viewed as a justifiable inroad into the principle of technology-neutral legislation in this context, because wrongful access is very proximate to the full offence.

However, the subsection is 'buggy' because it has the potential to over-criminalise a wide range of behaviour. *Watchorn* mentioned that "on the facts of *Dixon* [i.e. the copying of a video

---

[177] "Computer repair man's offending 'disturbing and sinister'" (26 March 2010) Stuff.co.nz <http://www.stuff.co.nz/national/crime/3511791/Computer-repair-mans-offending-disturbing-and-sinister>

[178] A prominent example of this is *United States of America v Dotcom* DC NS CRI-2012-092-001647, 23 December 2015 at [493], and [606]-[609]. Megaupload was a computer system that was used to infringe copyright – which constituted sufficient evidence of a breach of s 249.

[179] Crimes Act 1961, s 232

[180] Crimes Act 1961, s 72(1)

[181] United Kingdom Law Commission, *Report 186: Computer Misuse* (London, 1989) 25 at [3.52]. Their version of the provision is Computer Misuse Act 1990 (UK), s 2.

[182] Above n 145 at 18: the "rationale [t]here is that the police shouldn't have to wait for actual harm to occur." (The provision is Canadian Criminal Code RSC 1985 c 46 s 342.1(1)(c)).

[183] Above n 79 at 446

file],[184] it may be arguable that Mr Dixon was in breach of s 249(2) as well".[185] This illustrates the idea that mere access is all that is required to fulfil the elements of this subsection. This is because it could be used to avoid the general requirements of proximity under s 72, where a more proximate act might be required – such as searching for the video file to copy, but not actually doing so.

A good 'bug fix' here would be the complete removal of the subsection: Scotland's Law Commission, for example, has specifically deemed that such offending is best left to the general law of attempt,[186] and Australia has excluded the ability to charge for an inchoate offence of this type altogether.[187] The general law of attempt has been used for an offence under s 249(1) in New Zealand, in *Reddy v Police,* without any apparent difficulty.[188]

[184] See above n 99 for these.
[185] Above n 143 at [66]
[186] Scottish Law Commission *Report on Computer Crime* (Scot Law Com No 106, Edinburgh, 1987) at 20
[187] Criminal Code Act 1995 (Cth), s 477.1(8)
[188] *Reddy v Police* [2013] NZHC 2196 [28 August 2013]. The defendant changed her sister's online banking password and then attempted to transfer $20,000 to herself.

C Section 250

250 Damaging or interfering with computer system

(1) Every one is liable to imprisonment for a term not exceeding 10 years who intentionally or recklessly destroys, damages, or alters any computer system if he or she knows or ought to know that danger to life is likely to result.

(2) Every one is liable to imprisonment for a term not exceeding 7 years who intentionally or recklessly, and without authorisation, knowing that he or she is not authorised, or being reckless as to whether or not he or she is authorised,—

(a) damages, deletes, modifies, or otherwise interferes with or impairs any data or software in any computer system; or

(b) causes any data or software in any computer system to be damaged, deleted, modified, or otherwise interfered with or impaired; or

(c) causes any computer system to—

(i) fail; or

(ii) deny service to any authorised users.

The crux of this section is the protection of the integrity of the computer system, by criminalising damage to its function or to the data that it contains.

Paragraph 250(2)(c) is the central provision, and penalises causing the failure of a computer system. It is perhaps the 'archetypal' example of protection of amenity interests of computer systems: before all else, they must be 'up and running'.

In a similar vein to how s 249 should operate – criminalising 'wrongful access plus consequential further loss' – s 250(1) criminalises 'damage plus danger to life'. This is the 'most serious' of the offences, its maximum penalty being ten years' imprisonment. An example of its use might be where there is damage to the computer system controlling a car,[189] or (more dramatically) the computer system managing a nuclear reactor.[190] No case law

[189] For an example of where it might arise: see Andy Greenberg "Hackers Remotely Kill a Jeep on the Highway—With Me in It" (21 July 2015) Wired.com <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>.

[190] See above n 128 for discussion of the Stuxnet virus, which affected nuclear reactors in Iran (though not to cause meltdowns).

examining that subsection has been found in New Zealand, or examining similar provisions seen in Canada[191] and the United Kingdom.[192]

1 'Damage'/'deletion' of software or data in (2)

Subsection (2) does not only criminalise situations where computer systems fail: it also penalises the deletion of data. Such deletions, by implication, would not damage the integrity of computer systems as much as causing their complete failure under (c).

However, this section treats these different 'levels' of offending as equivalent and subjects them to the same maximum penalty of seven years' imprisonment. This is a 'bug' because it does not sufficiently distinguish between the different types of "damage" or "impairment" that might occur.

The amenity interests of computer systems do include the availability of the data on them, and users' trust in the integrity of that data. The Budapest Convention refers to computer data in isolation,[193] as does the United Kingdom statute when it refers to the impairment of "any such program or the reliability of any such data".[194]

However, deleting an assignment a friend is completing on her computer would constitute damaging data (an 'integrity' amenity interest). This will almost always be serious in nature than causing the failure of that computer system (an 'availability' amenity interest): for example, by deleting a file that was critical to the running of the "Windows" operating system, rendering her unable to use her computer at all.

Deletion of data within computer systems can also occur within employment situations, and so the inclusion of 'data' can cause the wording to extend to breaches of private duties. Section 250 charges were seen in *Police v Robb*,[195] where the defendant "deleted data in a computer system" by removing all of the files on his employer's hard drive,[196] and in *Vulcan Steel Ltd. v McDermott*,[197] where the defendant had deleted "at least two important emails relating to a substantial tender process", then failed to advise his employer of the existence of the tenders.[198]

Therefore, some form of recognition of the different 'levels' of offending might be appropriate in this section.

---

[191] Canadian Criminal Code RSC 1985 c 46, s 430(2)
[192] Computer Misuse Act 1990 (UK), s 3ZA
[193] Above n 42, arts. 4-6
[194] Computer Misuse Act 1990 (UK), s 3(2)(c)
[195] *Police v Robb* [2006] DCR 388. The case mainly turned on the question of the *mens rea* requirement of s 250, in terms of whether the defendant's deletion/wiping of the data was intentional.
[196] Above n 195 at [17]
[197] *Vulcan Steel Ltd. v McDermott* [2013] NZHC 3232
[198] Above n 197 at [31]

D Section 251

251 Making, selling, or distributing or possessing software for committing crime

(1) Every one is liable to imprisonment for a term not exceeding 2 years who invites any other person to acquire from him or her, or offers or exposes for sale or supply to any other person, or agrees to sell or supply or sells or supplies to any other person, or has in his or her possession for the purpose of sale or supply to any other person, any software or other information that would enable another person to access a computer system without authorisation—

(a) the sole or principal use of which he or she knows to be the commission of an offence; or

(b) that he or she promotes as being useful for the commission of an offence (whether or not he or she also promotes it as being useful for any other purpose), knowing or being reckless as to whether it will be used for the commission of an offence.

(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 an offence.

This section prohibits selling, distributing, or possessing software or information that would enable a computer criminal to undermine amenity interests by gaining "access [to] a computer system without authorisation". For example, lists of user credentials that have been gained in a major hack[199] indicate either past offending, future offending, or both.[200]

Very few charges under s 251 have been laid.[201] This is not unusual, however: offences of possession are generally difficult to investigate on their own.[202] However, as well as the potential of the wording to 'over-criminalise', there are also general criminal law considerations here regarding offences of possession. The idea of criminalising mere

[199] See, for example, the PlayStation Network hack, described above n 15

[200] Andrew Ashworth *Positive Obligations In Criminal Law* (Hart Publishing, Oxford, 2013) 149, paragraph [6.1]) categorises offences of possession in this way: 'prospective' offences (where the possession indicates a possible future crime) and 'retrospective' offences (where the possession indicates that a past crime has taken place).

[201] *R v Owen Thor Walker* HC HAM CRI 2008-075-711, 15 July 2008 is a rare example, where the defendant was found with malicious software on his computer. However, the Court did not discuss the software in any particular detail.

[202] For example, in the case of *Wardle v R* [2015] NZHC 915 at [3].

possession is that it is somehow indicative of a full offence, to the degree of making that possession criminal.[203] However, care must be exercised, because such offences criminalise mere preparatory acts at a point that is too remote from a full offence to provide an evidential basis for a charge related to it.

The speed of computer systems means that distributing such software, or using it to commit a crime, could take a matter of seconds and a few keystrokes. In this way, s 251 might be seen in a similar light to s 249(2) as protecting against 'particularly proximate' behaviour.[204] However, no amenity interests have been damaged by this possession: the damage to confidentiality interests from the possession of software that could be used to hack, for example, is only prospective.

There is also a need for recognition that the possession of such software can be for legitimate purposes.[205] The equivalent United Kingdom provision does not include the wording "sole use":[206] this caused the defendant in the United Kingdom case *R v Martin* to be charged with the possession of such software.[207] New Zealand's inclusion of the idea that the "sole or principal use" of the possessed software must be illegitimate provides this protection in paragraph (a), but not (b), which is a bug.

Concern can also arise about the inclusion of the phrase "information", which is a concept that can incorporate a computing context, but operates much more widely – to events such as email provider "Yahoo", in 2016, emailing its users to inform them of a data breach.[208] "Data" would incorporate the tools of computer crime (such as lists of hacked passwords), while avoiding any concerns about free flows of information. It is also the phrase used in Australia.[209]

Possession of "software or information" is also a property law concept, which is not an appropriate paradigm for this type of offending. Before *Dixon*, it was also not considered that "information" could be property, making it an intriguing drafting decision in that regard.

---

[203] Above n 200 at 49, 149

[204] Above n 79 at 444-445, Ashworth also makes this point. "Crimes of possession are…essentially inchoate: it is not the mere possession, so much as what the possessor might do with the article or substance, which is the reason for criminalisation."

[205] See, for example, Fahmida Y. Rashid "Cyber criminals cash out using PowerShell, other legitimate tools" (8 February 2016) InfoWorld <http://www.infoworld.com/article/3030689/security/cyber-criminals-cash-out-using-powershell-other-legitimate-tools.html>

[206] Computer Misuse Act 1990 (UK), s 3A. This was not received well by the information technology industry: see, for example, Graeme Wearden and Tom Espine "UK law will criminalise IT pros, say experts" (19 May 2006) ZDNet <http://www.zdnet.com/article/uk-law-will-criminalise-it-pros-say-experts/>.

[207] *R v Lewys Stephen Martin* [2013] EWCA Crim 1420 at [10]. One of the offences he was charged with regarded his use of 'CyberGhost,' a program for accessing the Internet anonymously.

[208] Seth Fiegerman "Yahoo says 500 million accounts stolen" (23 September 2016) CNN Money http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/>

[209] Criminal Code Act 1995 (Cth), s 478.4(1)(a)

III Level of Criminality: Sentencing

Where there is sufficient damage to the amenity interests of the computer system to attract liability under ss 248-252 (and the offending is not *de minimis*), the next stage will be an assessment of the level of that criminality through sentencing. This should encompass two things: that the harm caused by the offending be the primary consideration, and that the sentence should have a technology-neutral starting point.

In this context, harm can be expressed in terms of the damage caused to the integrity, availability, and confidentiality of computer systems – and any harm consequential upon this, such as financial or emotional harm. Where a computer system has genuinely made the offending more serious, it should be included as a factor in sentencing, but it should not be a starting point.

A Legislative: Maximum Penalties in Statute

Aside from s 252, the general scheme of New Zealand's statute is technology-neutral. Aside from s 250, the maximum available sentences are similar to those seen in other jurisdictions.

1 Section 249

Other jurisdictions have slightly different versions of this offence, so a sentencing comparison is difficult. Australia's 'further wrongful act upon unauthorised access', for example, is any offence that is punishable by more than five years' imprisonment. The maximum penalty under their provision is the maximum penalty for that other offence.[210] The United Kingdom's equivalent maximum is five years' imprisonment[211] and Canada's is ten years'.[212]

The best that can be said, in the face of this variation, is that the penalty for the 'subsequent wrongful offence' informs the maximum penalty for its 'computer crime version'. On this standard, the New Zealand sentence is at approximately the right level. The maximum penalty for committing an offence under s 249 is seven years' imprisonment, which is consistent with similar crimes in New Zealand. These include theft, if the value of the thing stolen exceeds

[210] Criminal Code Act 1995 (Cth), s 477.1(6)
[211] Computer Misuse Act 1990 (UK), s 2(5)(c)
[212] Canadian Criminal Code RSC 1985 c 46, s 342.1

$1000;[213] receiving stolen goods;[214] and other 'theft-like' offences.[215] Therefore, our level is appropriate, and alteration is not required.

2 Section 250

Section 250 and its physical-property equivalent, "Intentional damage", have maximum sentences of ten years' imprisonment for danger to life, or seven years' for other general cases of damage.[216] This is comparatively light, amongst similar provisions in other jurisdictions. Australia[217] and the United Kingdom[218] have a maximum penalty of ten years' imprisonment for the 'general damage' provision. Canada's 'danger to life' provision has a maximum sentence of life imprisonment,[219] and 14 years' in the United Kingdom.[220]

New Zealand's maximum penalty should therefore be increased in cases where there is serious damage to amenity interests. The failure of the software that controls a car's steering could have very serious consequences, especially because it could occur on all cars of that model.

This would mean that the penalty would not be technology-neutral. However, the computer system context is inherently different here, because the central component of the protection of amenity interests of computer systems is their availability. Even if danger to life does not result, the fact still remains that s 250 is the most serious offence of the four: this should be reflected in statute.

3 Section 251

The maximum sentence here is two years' imprisonment, which 'fits' well with our statute and those of other jurisdictions. Similar provisions in the Act generally carry a maximum sentence of either two or three years' imprisonment:[221] comparing with other jurisdictions, Australia's

[213] Crimes Act 1961, s 240
[214] Crimes Act 1961, s 246
[215] Others include "Money laundering" (s 243), "Theft by person in special relationship" (s 220), and "Criminal breach of trust" (s 229).
[216] Crimes Act 1961, s 269, subss (1) and (2)
[217] Criminal Code Act 1995 (Cth), ss 477.2 and 477.3
[218] Computer Misuse Act (UK), s 3(6)
[219] Above n 191
[220] Computer Misuse Act (UK), s 3ZA(6)
[221] Crimes Act 1961, s 272 (2 years' imprisonment) "Providing explosive to commit crime": see also s 233 (3 years') "Being disguised or in possession of instrument for burglary". The Summary Offences Act offences' average (see below heading "Section 252" at page 53) is closer to three months' imprisonment, but those offences are implicitly less serious because of the statute they appear in.

maximum penalty is three years' imprisonment,[222] while the United Kingdom[223] and Canada's[224] are two years'. This means alteration of the sentence is not necessary.

4 Section 252

This section is the only one of the four that is penalised at a notably higher level than its 'real-world' counterpart (trespass), with a maximum of two years' imprisonment. Criminal trespass is a summary offence, with a maximum term of imprisonment of three months.[225]

However, s 252 was inserted as a criminal offence during the legislative passage of the Amendment Act,[226] even though the first draft in 1989 recommended that it be a summary offence and have a lower penalty of six months' imprisonment.[227] In terms of legislative intent, it can therefore be seen as 'more serious' than trespass, in the same way that s 251 has a higher penalty than comparable offending in the Summary Offences Act.[228] It is also similar to comparable jurisdictions: the United Kingdom has the same maximum penalty,[229] for example, as does Australia.[230]

The rationale for a higher penalty was described in *Silva*: that[231]

> *when one considers the fact that there is a two year prison sentence which is imposable in matters of this nature… [the Court must take into account] the reliance that all of us place on computers these days and their security.*

This is, therefore, an example of a justified departure from the goal of technology-neutral legislation. The fact of unauthorised access is, on its own, a serious erosion of computer systems' confidentiality and integrity amenity interests – more so than trespass. Therefore, a change is not required.

---

[222] Criminal Code Act 1995 (Cth), ss 478.3 and 478.4
[223] Computer Misuse Act (UK), s 3A(5)(c)
[224] Canadian Criminal Code RSC 1985 c 46, s 342.2(1)(a)
[225] Trespass Act 1980 s 11(2)(a)
[226] Above n 43
[227] Above n 31 at 77
[228] See Summary Offences Act 1981, s 14 "Possession of burglary tools", s 13A "Possession of knives", and s 13B "Possession of high-power laser pointers": all of which have a maximum available penalty of six months' imprisonment.
[229] Computer Misuse Act (UK), s 1(3)(c)
[230] Criminal Code Act 1995 (Cth), s 478.1
[231] Above n 103 at [16].

B Judicial: Hayes

The wording of the statute is only one factor in sentencing: the other is judges' utilisation of it in practice. In *Hayes*, the Court of Appeal gave a well-considered indication of how judges can go about this process,[232] and it has been cited in many cases since.[233]

The Court focused closely on the harm caused by the offender, in terms of the diminishing of the amenity interests of computer systems and the other interests that they protect. These included the loss suffered, the emotional impact of the offending, and the number of people and computer systems that were affected. The harm done to wider amenity interests (such as public confidence in computer systems[234]), the goal of legislation being technology-neutral,[235] and other relevant considerations (such as moral wrongfulness) were all also emphasised.[236]

[232] *R v Mark Hayes*, above n 61. The defendant, in that case, was charged under s 249. He had devised a scheme to buy electronic goods on TradeMe with funds he appropriated with stolen online banking credentials: he also installed software to track keyboard input, which allowed him to gain people's online banking passwords.
[233] See, for example, *R v Owen Thor Walker* above n 201 at [21], *Whitaker v Police* above n 168 at [23], and *Sarah v R* (CA) above n 173 at [15]-[16].
[234] At [76].
[235] At [77].
[236] These included the prospect of other, future, offending at [76]. In the context of the Sentencing Act, relevant criteria included accountability for harm, denouncing of the conduct, deterrence, extent of harm, abuse of position of trust, premeditation, and previous convictions: s 7(1)(a), (e) and (f) and s 9(1)(d), (f) and (i) and (j) of the Sentencing Act 2002.

IV Conclusion

For ss 248-252 to be functional and effective, they must be precisely worded in a way that is as narrow as possible. This wording should focus on the protection of amenity interests, as should the process of interpreting it.

The case law containing such interpretations is not plentiful, and much of it is in the form of sentencing decisions: these are less likely to involve a substantive analysis of the elements of the offences. However, there is sufficient case law to find bugs in the statute.

The most troubling of these is s 249, which penalises the specific offence of the use of a computer system to a wrongful end; this bug carries over to its subsection (2). Section 250 has been utilised as a very serious charge where the level of offending is low: however, its maximum penalties should be raised. These are competing, but not irreconcilable, objectives. There is also a need for narrower definitions of "authorisation" and "computer system", which are more focused on the protection of amenity interests, in s 248; and also for more 'finely calibrated' definitions in s 251.

However, overall, the 'program' of New Zealand's statute is mostly well-implemented and functional. Where bugs have been found, 'fixes' for all of them are found below in Chapter III.

Chapter III: Adjustments and Additions

The offences under ss 248-252 generally provide good ‘coverage’ of the types of computer crime that might occur. However, they extend beyond protection of amenity interests at points, especially in s 249.

This chapter consists of ‘marked-up’ suggested changes to ss 248-252, to attempt to fix these bugs, paying regard to the earlier discussion in Chapter II and the schemes seen in other jurisdictions.

I Sections 248 and 252

248 Interpretation

For the purposes of this section and sections 249 to 252, –

access, in relation to any computer system, means instruct, communicate with, store data in, receive data from, or otherwise make use of any of the resources of the computer system**.**

authorisation **—**

(a) includes an authorisation conferred on a person by or under an enactment or a rule of law, or by an order of a court or judicial process**; and**

(b) remains valid if a person who is authorised to access a computer system does so for –

(i) a purpose other than the one for which that person was originally given authorisation; or

(ii) in breach of any condition, express or implied, that access was granted contingent upon.

The idea of what a “computer system” is, and related ideas of how one might be “authorised” to “access” it, could include profoundly different technologies five years from now. Prediction of the form of these technologies is difficult: in 1945, a technology magazine wrote

"…computers of the future may have only 1,000 vacuum tubes and perhaps weigh one and a half tons."[237]

The legislation covering them should, then, be as broad as possible to 'keep pace' with technological development. However, the correlating 'bug management strategy' here is the need to avoid 'over-criminalising' offending where possible. This can be done by using language that specifically only protects amenity interests, and by utilising a purposive approach in statutory interpretation.

A "Authorisation"

"Authorisation" is a very context-based concept, and when it is lost will require intensive examination on a case-by-case basis. Civil duties are relevant, but it would be inappropriate for computer crime law to extend to the point of penalising their violation. Employees that already have access but use it for the 'wrong' purpose, such as overpaying themselves[238] or using Facebook during working hours, do not diminish the amenity interests of computer systems.

The Explanatory Note to the Amendment Act shows legislative intent that employees' access of *other* computer systems (without authorisation) be criminal:[239] some commentators claim that this leaves a 'loophole' in s 252(2), where employees use their legitimate access to an 'internal' computer system improperly. Taking an approach based on the diminishing of amenity interests, however, the opposite is true: civil law causes of action (like employment law) should be used instead. The defence does not extend far enough, and this means there are two bugs that need fixing.[240]

Firstly, the exemption under s 252(2) should apply to the provisions generally, similarly to the scheme seen in Australia:[241] this is implemented in s 248 in the box above as paragraph **(b)(i)**.

Secondly, the statute does not expressly indicate whether an actual *breach* of the terms that access was granted upon will be unauthorised. There has been legislative impetus in the United

---

[237] Kevin Fogarty "Tech predictions gone wrong" (22 October 2012) ComputerWorld <http://www.computerworld.com/article/2492617/it-management/tech-predictions-gone-wrong.html>

[238] See above n 168, for a sample of s 249 cases that involved this type of offending.

[239] Above n 43

[240] For more discussion of why this is so, see the above heading "Removal of the exception in s 252(2)?", on page 37.

[241] Criminal Code Act 1995 (Cth), s 476.2: unauthorised is defined as "where the person is not entitled to cause that access, modification or impairment" and – similarly to s 252(2) – a person's conduct "is not unauthorised merely because he or she has an ulterior purpose for causing it."

States to add a statement that it is not, following troubling case law on that question.[242] To make this explicit in New Zealand, a similar provision has been inserted above as **(b)(ii)**.

B "Computer System"

248 Interpretation

[…]

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

(a) **contains computer programs and other computer data, and**

(b) by means of computer programs,

(i) performs logic and control, and

(ii) may perform any other function.

~~(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 communication facilities, and stored data.~~

Amenity interests are provided by a computer system in operation, which constitutes the interaction of software and data on hardware. However, the focus of this wording is 'buggy' in that it is not sufficiently targeted at the protection of amenity interests.

The term 'computer' is not defined in the United Kingdom[243] or Australia,[244] leaving the question as a fact-based one. However, this could be too wide, because the forms a 'computer' can take are infinite. The definition would be improved if it specifically focused on the amenity interests provided by the computer system. The wording of the Budapest Convention does this

[242] H.R. 2454 (113th): Aaron's Law Act of 2013. The Bill has stalled amongst Congressional gridlock. For more, see Kieren McCarthy "'Aaron's Law' back on the table to bring sanity to US hacking laws" (23 April 2015) The Register <http://www.theregister.co.uk/2015/04/23/congress_reintroduces_aarons_law/>

[243] Computer Misuse Act (UK)

[244] Criminal Code Act 1995 (Cth)

by describing the central relevant components: programs and data.[245] Countries such as Singapore[246] and Canada[247] follow a similar approach.

The Canadian wording, especially, describes the holistic computer system in operation. In the portion inserted above as paragraph **(a),** these dual components of programs and data are included.[248] Paragraph **(b)** then describes the interactions between them: **(b)(i)** entails the use of logical operations (computer programs) that control and manipulate data, **(b)(ii)** describes all of the auxiliary functions that this entails.

The United States is one country that lists exemptions to their definition of a computer: "an automated typewriter or typesetter, a portable hand-held calculator, or other similar device".[249] This can be seen as a statutory 'floor' on the types of computer systems that can incur liability for being interfered with. However, New Zealand courts (as cases such as *Boyack*[250] have shown) appear to be interpreting the statute with a *de minimis* approach in mind already, so it is not currently necessary.

C "Access"

> 248 Interpretation
>
> […]
> *access*, in relation to any computer system, means instruct, communicate with, store data in, receive data from, **intercept**, or otherwise make use of any of the resources of the computer system

The recommendations of the Law Commission,[251] the wording in some other jurisdictions,[252] and the Budapest Convention[253] also suggest specific criminal sanctions for the 'interception' of communications between computer systems: this would further protect the 'confidentiality' element of their amenity interests. However, it may not be necessary. Canada's inclusion of

[245] Above n 42 at art. 1: "any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data'".
[246] Computer Misuse Act 1998 (Singapore), c 50A s 2
[247] Canadian Criminal Code RSC 1985 c 46, s 342.1(2)
[248] As a minor change, to reflect this 'holistic' nature, 'or' has been replaced by 'and' in the phrase "contains computer programs and other computer data."
[249] 18 USC § 1030(e)(1)
[250] Above n 125
[251] Above n 39 at 28, [90]
[252] See, for example, the Canadian Criminal Code RSC 1985 c 46, s 342.1(1)(b)
[253] Budapest Convention, above n 42, art. 3

‘interception’, for example, is defined as “listen to or record a function of a computer system…”:[254] such acts of unauthorised interception would surely first require unauthorised access. This could be made more explicit, however, and is inserted above.

[254] Canadian Criminal Code RSC 1985 c 46, s 342.1(2)

II Section 249

249 **Accessing computer system without authorisation, and obtaining a benefit or causing loss** ~~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 **without authorisation, knowing that he or she is not authorised, or being reckless as to whether or not he or she is authorised,** 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**;**

~~(2) Every one is liable to imprisonment for a term not exceeding 5 years who, directly or indirectly, accesses any computer system with intent, dishonestly or by deception, and without claim of right,~~

~~(a) to obtain any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or~~

~~(b) to cause loss to any other person.~~

(**2**~~3~~) In this section, *deception* has the same meaning as in section 240(2).

If an employee physically takes cash out of a till and also makes unsanctioned online bank transfers to herself, she has *prima facie* committed theft in both scenarios. However, her use of the computer system in the second opens her up to two separate forms of liability, the second being s 249. If she merely starts up her computer with the intent to do so, she could also attract liability under s 249(2).

The first bug here is that the statute penalises *any* access with a dishonest purpose. It implicitly and unjustifiably 'heightens' the offending because a computer was used in its commission, and so is not technology-neutral. It should instead be focused on the protection of amenity interests, and of other interests they might affect (such as financial ones).

The fix for this major bug is a minor one, however. Addition of 'unauthorised' is the best course of action, by copying the relevant wording from s 252 into **(1)** above: this would make this offence a 'more serious' version of s 252. The scheme would then correspond with the Law

Commission's initial recommendations for the statute,[255] and with provisions seen in other jurisdictions.

The second bug is the scope of subsection **(2).** The Act and the general criminal law can sufficiently address attempts under s 249, without this specific provision for it. Therefore, it should be removed altogether: the offending is not so proximate to justify a separate offence with a high maximum sentence.

A Widening of the Subsequent Offence?

> 249 **[**Accessing computer system without authorisation, and obtaining a benefit or causing loss**]**
>
> (1) Every one is liable to imprisonment for a term not exceeding 7 years who, directly or indirectly, accesses any computer system **[**without authorisation, knowing that he or she is not authorised, or being reckless as to whether or not he or she is authorised,**]** and thereby, dishonestly or by deception, and without claim of right,—
>
> […]
>
> **(c) commits any offence that is punishable by more than five years' imprisonment.**

The criminal acts committed after the access, in s 249(1)(a)-(b), are all related to material interests: this scheme was likely intended to make the section congruent with other offences in this Part of the Act, which focuses on "rights of property".[256]

However, this may be too narrow: computer systems do not only protect financial interests. The data they contain can also be private, or have sentimental value.[257] The Court in *Police v Le Roy*, however, held that the definition of 'benefit' was not "confined to a benefit of a financial or pecuniary nature" and could extend to the ability of the defendant to access the

[255] Above n 62

[256] That part being "Crimes against rights of property." See for example Crimes Act 1961 s 240(1): "(a) obtains ownership or possession of, or control over, any property, or any privilege, service, pecuniary advantage, benefit, or valuable consideration, directly or indirectly […] (d) causes loss to any other person."

[257] Hayes recognised this idea, holding that emotional forms of harm were relevant to sentencing: above n 61 at [76].

email messages of his ex-wife.[258] If Courts are already willing to extend the definition to non-property interests, extension may not be necessary.

Privacy law also protects these interests: the addition of a criminal law sanction might further confuse an area of law that is already somewhat of a 'patchwork'[259] and is largely civil in nature.[260] The Select Committee report on the Amendment Act also rejected submissions suggesting it add an offence of this type.[261]

However, the fact remains that the list in s 249(1)(a)-(b) puts New Zealand 'out of step' with other countries. In the United Kingdom[262] and Australia,[263] the provision applies to any offence with a maximum penalty of more than five years' imprisonment.[264] This may be a good 'middle ground' addition, better reflecting that confidentiality and amenity interests are also very important in this context. Consider a 2014 example, where intimate photos of celebrities were released online in a very harmful breach of privacy: this was effected using illegitimate access to their computer systems.[265]

[258] *Police v Le Roy* HC WN CRI-2006-485-38, 31 July 2008 at [21]
[259] For a description of this 'patchwork', see Law Commission *Privacy Concepts and Issues: Review of the Law of Privacy Stage 1* (NZLC SP19, 2008) at 70
[260] See the Privacy Act 1993. There are some available criminal sanctions, such as Part 9A of the Act ("Crimes against personal privacy"), and ss 21-22 of the Harmful Digital Communications Act 2015.
[261] Above n 43 at 19: the offence was phrased "unauthorised access with intent to commit further offences."
[262] Computer Misuse Act (UK), s 2(2)(a)
[263] Criminal Code Act 1995 (Cth), s 477.1(d)
[264] The Budapest Convention provides only the option to add this type of offending: at above n 42 art. 2: "A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent…"
[265] The photos in question were obtained through illegitimate access of users' iCloud accounts. For more, see Charles Arthur "Naked celebrity hack: security experts focus on iCloud backup theory" (1 September 2014) The Guardian Online <https://www.theguardian.com/technology/2014/sep/01/naked-celebrity-hack-icloud-backup-jennifer-lawrence>

III Section 250

250 Damaging or interfering with computer system

(1) Every one is liable to imprisonment for a term not exceeding ~~10~~ **14** years who intentionally or recklessly destroys, damages, or alters any computer system if he or she knows or ought to know that danger to life is likely to result.

(2) Every one is liable to imprisonment for a term not exceeding ~~7~~ **10** years who intentionally or recklessly, and without authorisation, knowing that he or she is not authorised, or being reckless as to whether or not he or she is authorised,—

(a) damages, deletes, modifies, or otherwise interferes with or impairs any data or software in any computer system**,**

(i) in a way that substantially impairs its ability to function properly; or

(ii) that thereby causes serious damage to infrastructure, or serious loss to any other person, or;

~~(b) causes any data or software in any computer system to be damaged, deleted, modified, or otherwise interfered with or impaired; or~~

(c**b**) causes any computer system to—

(i) fail; or

(ii) deny service to any authorised users.

(3) Every one is liable to imprisonment for a term not exceeding 2 years who intentionally or recklessly, and without authorisation, knowing that he or she is not authorised, or being reckless as to whether or not he or she is authorised,—

(a) damages, deletes, modifies, or otherwise interferes with or impairs any data or software in any computer system; or

(b) causes any data or software in any computer system to be damaged, deleted, modified, or otherwise interfered with or impaired.

‘Damage’, in a physical-property context, might entail breaking a wing mirror off a stranger’s car.[266] In a computer-system context, it might entail ‘overloading’ it with requests so as to make it inaccessible to other users.[267]

This section is cogently worded, and similar to other versions of it in other jurisdictions. However, while our maximum available penalty is too low in a comparative sense, it is too high in a purposive sense. With regards to the first, the maximum penalties have been changed to 14 and 10 years’ imprisonment in **(1)** and **(2)** respectively: this is the scheme from the United Kingdom.[268] With regards to the second, though, s 250 has been extended to use in employment disputes. A high maximum penalty is inappropriate where such private duties were breached but amenity interests were not violated to a high degree.

Another section of the Act, “Punishment of theft”,[269] can provide a suggestion of how to simultaneously fix both bugs. It uses a ‘tiered’ penalty structure, categorising the loss by the value of what was stolen (greater than $1000, less than $500, or somewhere in between).[270] A similar ‘stepwise’ scheme could be enacted for this situation: this would also be similar to the scheme in Australia, which provides different versions of this offence which vary by ‘seriousness’.[271]

The first ‘step’, **(2)** above, reserves the highest available penalty for the damage to the ‘availability’ amenity interest: computer systems, first and foremost, need to be available for use. The United Kingdom also goes beyond the role of s 250(1) as protecting against “danger to life” by also allowing for “damage to infrastructure.”[272] This could be included as part of **(2)(a)(ii)**.

The second ‘step’, **(3)**, will then allow for a ‘lesser version’ of the offence if only other amenity interests are affected – such as integrity of data, or trust in functionality. These amenity interests are broadly analogous to those affected by s 252. Therefore, the same maximum penalty as s 252, two years’ imprisonment, has been inserted: this also correlates with the Australian maximum.[273]

[266] Criminalised by s 269 of the Act, “Intentional damage”.
[267] Generally referred to as a ‘denial-of-service attack’: see above n 13 for further discussion of this.
[268] Computer Misuse Act 1990 (UK), ss 3(6) (10 years’ imprisonment) and 3ZA(6) (14 years’).
[269] Crimes Act 1961, s 223
[270] As well as whether the defendant was in a special relationship (s 220) with the complainant, per s 223(a).
[271] Criminal Code Act 1995 (Cth), ss 477.2 and s 477.3 c.f. ss 478.2 and 478.3.
[272] Computer Misuse Act 1990 (UK), s 3ZA(7)
[273] Criminal Code Act 1995 (Cth), ss 478.2 and 478.3.

IV Section 251

251 ~~Making, s~~**S**elling, ~~or~~ distributing**,** or ~~possessing~~ **having** software for committing crime

(1) Every one is liable to imprisonment for a term not exceeding 2 years who invites any other person to acquire from him or her, or offers or exposes for sale or supply to any other person, or agrees to sell or supply or sells or supplies to any other person, or has ~~in his or her possession~~ for the purpose of sale or supply to any other person, any software or ~~other information~~ **data** that would enable another person to access a computer system without authorisation—

(a) the sole or principal use of which he or she knows to be the commission of an offence; or

(b) that he or she promotes as being useful for the commission of an offence (whether or not he or she also promotes it as being useful for any other purpose), knowing or being reckless as to whether it will be used for the commission of an offence.

(2) Every one is liable to imprisonment for a term not exceeding 2 years who ~~has in his or her possession~~**has** any software or ~~other information~~ **data** that —

(a) would enable him or her to access a computer system without authorisation; and

(b) its the sole or principal use is the commission of an offence; and

(~~b~~**c**) **he or she** intends to use **it** ~~that software or~~ ~~other information~~ to commit an offence.

Envision that a prospective computer criminal wants to find a flaw in a computer system, so they can exploit it and hack in. If they are not skilful in that art, they can purchase an 'exploit kit', which is a piece of software that will find the flaws for them. This is this type of situation that s 251 guards against.

This section was not discussed at great length by the Select Committee when they recommended its insertion; the increasing prominence of 'tools of computer crime',[274]

[274] Lillian Ablon, Martin C. Libicki, Andrea A. Golay *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar* (RAND Corporation, California, 2014) at 29.

however, makes it a very prescient addition in hindsight. A report on the matter states that there exist *bona fide* 'black markets' for such 'means' of computer crime.[275] It also found that they have grown, and will continue to do so.

There are minor bug fixes available in this section, that better calibrate it to the protection of amenity interests: removing the property law concept of "possession",[276] replacing "information" with "data", and adding "sole and principal use" as **(2)(b)**. Similarly to s 249(2), the title is also not descriptive of the elements of the offence: "making", accordingly, has been removed.

> 251 Selling, or distributing, or having software for committing crime
>
> […]
>
> **(3) It is not an offence to attempt to commit an offence under this section.**

Australia creates a statutory 'bar' to the charge of an inchoate offence under this section.[277] The offence of attempting to possess seems very proximate from the actual fact of offending: as a suggestion, their wording has been inserted above.

[275] Above n 274 at 1: "Black markets are organized and run for the purpose of cybercrime; they deal in exploit kits, botnets, Distributed Denial of Service (DDoS) attack services, and the fruits of crime (e.g., stolen credit card numbers [and] compromised hosts)".
[276] For more discussion of the use of property law in this context, see the above heading "'Computer-System-as-Target' Protection with Property Law?" at page 22.
[277] Criminal Code Act 1995 (Cth), ss 478.3(3) and 478.4(3)

V Addition of New Provisions

There are no obvious 'loopholes' or 'gaps' in what criminal acts are covered by ss 248-252.[278] However, the following are two possible 'extras' that merit mention, though the myriad issues surrounding them go beyond the scope of this work.

A Possession of Stolen Data

One of the goals in New Zealand's cyber-security policy document was "considering whether we need an offence of unlawful possession of stolen data."[279] This is slightly different from an offence of "wasting data", which the Select Committee decided not to implement in their report on the Amendment Act.[280]

After the Supreme Court decision in *Dixon*, which held that computer files can be considered property,[281] there is also the possibility that the act could be charged under the offence of 'receiving stolen goods'.[282]

Policy concerns regarding criminalising mere possession, similarly to s 251, exist here too: because it is a very simple matter to receive data in a computer context, the crime may be 'too easy' to commit. However, this does provide an option for prosecutions in an area where it can be very difficult to gather evidence. It should be in terms that are as narrow as possible if enacted, and should provide a high standard for determining that the data was obtained illegitimately.

B Civil Remedies

The United States allows civil claims in its computer crime statute.[283] In the United Kingdom, police have instituted a policy of passing the details of computer crimes on to private law firms, for them to pursue the actions in civil law.[284] With the lower burden of proof in a civil context, and the ability to gain compensatory recovery instead of reparations, an alternate civil scheme

[278] Concepts involved in the investigating of, and the procedure of prosecuting, computer crime – such as jurisdiction, telecommunications, warrants to 'eavesdrop', and forced data-breach notifications – are important, and are points of discussion in various policy documents (see the above heading "Policy responses" at page 12): however, they are beyond the scope of this work.
[279] Above n 21 at 12
[280] Above n 43 at 18
[281] Above n 99 at [51]
[282] Crimes Act 1961, s 246
[283] 18 USC § 1030(g)
[284] Vikram Dodd "Police to hire law firms to tackle cyber criminals in radical pilot project" (14 August 2016) The Guardian Online <https://www.theguardian.com/uk-news/2016/aug/14/police-to-hire-law-firms-to-tackle-cyber-criminals-in-radical-pilot-project>

might provide some relief for complainants in New Zealand. However, where there is one 'central area' that governs both the civil and criminal jurisdictions, the determination of whether actions are civil or criminal in nature can become blurred.

Courts in the United States have used other areas of the civil law – such as, problematically, the property law paradigm of trespass[285] – in cases involving the civil jurisdiction: these have also – again, problematically – 'carried over' at times to interpretation of the Act in a criminal context.[286]

[285] See Jennifer Granick, above n 150 at 24:46: <https://youtu.be/F4XdxmLUfqI?t=24m46s>
[286] See, for example, *LVRC Holdings v. Brekka* 581 F 3d 1127, 1135 9th Cir. (2009) at 13387

Conclusion

Computer crime law is a vital component of modern-day criminal law frameworks: it protects computer systems against the inevitable attacks they face as they become increasingly vital to the way that people live and work – both in New Zealand and globally. Criminal law is but one mechanism that is necessary to cope with this challenge, but it is an important factor.

The purpose of computer crime law – how we would like the 'program' of our statute to function – is to protect the amenity interests of computer systems. These are a *sui generis* public good, and constitute computer systems' integrity, availability, and confidentiality. Legislation needs to be broadly worded in this constantly-changing context: however, as far as is possible, it must be drafted and interpreted to fulfil this purpose.

This work has contended that, largely because of 'bugs' in ss 248-252, these offences have sometimes extended into areas beyond this intended purpose. For example, they have been used in disputes that are essentially private in nature, and where a computer was used as a 'tool' for other offending (a major bug in s 249). 'Bug fixes' were proposed to fix these in Chapter III.

A robust, 'healthy' framework that applies precisely and predictably is important: even though New Zealand is a small nation, it is not immune from computer crime. Robert Mueller, the director of the FBI, said in 2012: "There are only two types of companies: those that have been hacked, and those that will be."[287]

[287] "FBI Director: Hacking Will Replace Terrorism As The Nation's Top Worry" (2 March 2012) Business Insider Australia <www.businessinsider.com.au/robert-mueller-fbi-hacking-terrorism-2012-3?r=US&IR=T>

Bibliography

A Cases

1 New Zealand

Amanda Renee Spence and Dominic Stormy Visser v New Zealand Police HC ROT CRI-2007-077-001151, 25 February 2009

Appuhamilage v Police [2015] NZHC 2355

Ashby v Police [2015] NZHC 1900

Benjamin v R [2012] NZSC 39

Burt v Police [2012] NZHC 2551

Cai v R [2011] NZCA 604

Dixon v R [2015] NZSC 14, NZSC Trans 9: *R v Dixon* [2014] NZCA 329

Fisher & Paykel Financial Services v Karum Group [2012] NZHC 3314

Fitzmaurice v New Zealand Police [2013] NZHC 494

Gao v R [2013] NZCA 173

Herbst v The Minister of Immigration [2014] NZIPT 600088

ITE v ALA [2016] NZEmpC 42

Jackson v Serious Fraud Office [2012] NZHC 3297

Jardine v R [2016] NZCA 371

Le Roy v Police HC WN CRI-2008-485-58, 31 July 2008: *Police v Le Roy* HC WN CRI-2006-485-38, 25 August 2008

McLachlan v R [2014] NZCA 462

Murray v Wishart [2014] NZCA 461

New Zealand Police v Franciso Javier Correa Silva DC WN CRI-2010-085-007353, 10 December 2010

New Zealand Police v Whitaker [2015] NZDC 24887

Pacific Software Technology Ltd v Perry Group Software [2004] 1 NZLR 164

Police v Dick DC ROT CRI-2009-063-007025, 1 July 2010

Police v Greig DC Manukau, CRI 2004-092-003818, 24 May 2004

Police v Knight DC QUN CRI-2011-059-001363, 16 January 2012

Police v Robb [2006] DCR 388

R v Boyack [2008] HC Auckland CRI 2007-044-002515, 6 June 2008

R v Garrett [2001] DCR 955

R v Grygoruk HC AK CRI 2006-092-12831, 23 May 2008

R v Kerr DC WN CRI-2008-032-004266, 25 May 2009

R v Mark Hayes CA CA197/06, 24 November 2006

R v Marriner DC NWP CRI-2011-043-002852, 9 December 2011

R v Misiç [2001] 3 NZLR 1
R v Owen Thor Walker HC HAM CRI 2008-075-711, 15 July 2008
R v Wilkinson (1998) 16 CRNZ 179
Reddy v Police [2013] NZHC 2196
Sarah v R [2013] NZCA 446
Serious Fraud Office v Ross [2014] DCR 163
Singh v Serious Fraud Office HC AK CRI 2008-404-000361, 4 March 2009
Slater v APN New Zealand Ltd [2014] NZHC 2157
Thomas v New Zealand Police HC AK CRI 2008-404-343, 9 February 2008
United States of America v Dotcom DC NS CRI-2012-092-001647, 23 December 2015
Wardle v R [2015] NZHC 915
Watchorn v R [2014] NZCA 493
Whangapirita v Police [2012] NZHC 308

2 United Kingdom

Cox v Riley (1986) 83 Cr App R 54
DPP v Bignall [1998] 1 Cr App R 1
Force India Formula One Team Limited v Aerolab SRL & Anor [2013] EWCA civ 780
Oxford v Moss (1979) 68 Cr App R 183 (QB)
R v Gold and Schifreen [1988] 1 AC 1063 (HL)
R v Lewys Stephen Martin [2013] EWCA Crim 1420
R v Preddy, Slade and Dhillon [1996] UKHL 13
R v Whiteley (1991) 93 Cr App R 25

3 United States

LVRC Holdings v. Brekka 581 F 3d 1127, 1135 9th Cir. (2009)
United States v Aaron Swartz 1:11-cr-10260 (2011)
United States v O'Brien 435 F 3d 36 04-2447 (2006)
United States v. Drew 259 FRD 449 CD Cal (2009)
United States v. Neil Scott Kramer, 58 ALR Fed 2d 611 (2011)

B Legislation

1 New Zealand

Crimes Act 1908
Crimes Act 1961
Crimes Amendment Act 1973

Crimes Amendment Act 2003
Crimes Amendment Bill (No 6) 1999 and Supplementary Order Paper No. 85 (322-2)
Crimes Bill 1989 (152-1)
Criminal Procedure Act 2011
Harmful Digital Communications Act 2015
Privacy Act 1993
Sentencing Act 2002
Summary Offences Act 1981
Trespass Act 1980

2 International

Aaron's Law Act of 2013 H.R. 2454 (113th): (United States of America)
Canadian Criminal Code RSC 1985 c 46 (Canada)
Computer Misuse Act (United Kingdom)
Computer Misuse Act 1998 (Singapore)
Criminal Code Act 1995 (Cth) (Australia)
Forgery and Counterfeiting Act 1981 (United Kingdom)
United States Code, Title 18, Part I, Chapter 47, § 1030 (United States of America)

C Treaties and United Nations Materials

Council of Europe Convention on Cybercrime (opened for signature 23 November 2001, entered into force 1 July 2004)

United Nations Office on Drugs and Crime *Comprehensive Study on Cybercrime: Draft* (Vienna, 2013)

D Books

Ashworth, Andrew and Horder, Jeremy *Principles of Criminal Law* (7th ed., Oxford University Press, Oxford, 2013)

Ashworth, Andrew *Positive Obligations in Criminal Law* (Hart Publishing, Oxford, 2013)

Ashworth, Andrew *Principles of Criminal Law* (5th ed., Oxford University Press, Oxford, 2006)

Blackstone, William *Commentaries on the Law of England 1765-1769: Volume 2* (The University of Chicago Press, Chicago, 1979)

Bradley, Tony *Essential Computer Security: Everyone's Guide to Email, Internet, and Wireless Security* (Syngress, Massachusetts, 2006)

Ceruzzi, Paul *A History of Modern Computing* (2nd ed., MIT Press, Massachusetts, 2003)

Clough, Jonathan *Principles of Cybercrime* (2nd ed., Cambridge University Press, Cambridge, 2015)

Harvey, Judge David *internet.law.nz* (4th ed., LexisNexis New Zealand, Wellington, 2014)

Hepburn, Samantha *Principles of Property Law* (Cavendish Publishing, Great Britain, 1998)

Honoré, Anthony "Ownership" in Anthony Honoré *Making law bind: essays legal and philosophical.* (Clarendon Press, Oxford, 1961)

Miller, Steve *The Complete Idiot's Guide to the Science of Everything* (Penguin, London, 2008)

Reyes, Anthony, Brittson, Richard, O'Shea, Kevin, and Steele, James *Cyber Crime Investigations* (Syngress, Massachusetts, 2007)

Ziff, Bruce *Principles of Property Law* (6th ed., Carswell, Toronto, 2014)

E Chapters in Edited Books

Husak, Douglas "De Minimis 'Defence' to Criminal Liability" in R.A. Duff and Stuart Green (ed.) *Philosophical Foundations of Criminal Law* (Oxford Scholarship Online, 2011)

Robertson, Bruce and Finn, Jeremy (ed.) *Adams on Criminal Law: 2016 Student Edition* (Thomson Reuters, Wellington, New Zealand, 2016)

F Journal Articles and Dissertations

Allan, Gregor "Responding to Cybercrime: A Delicate Blend of the Orthodox and the Alternative" (2005) 2 NZ L Rev 149

Briggs, Assoc. Prof. Margaret "Criminal Law" (2013) 1 NZ L Rev 136

Clough, Jonathan "Data Theft? Cybercrime And The Increasing Criminalization Of Access To Data" (2011) 22 Crim L Forum 145

Dagan, Hanoch "The Craft of Property" (2003) 91 Cal L Rev 1517

Decker, Charlotte "Cyber Crime 2.0: An Argument To Update The United States Criminal Code To Reflect The Changing Nature Of Cyber Crime" (2008) 81(5) S Cal L Rev 959

Green, Lance "Does The Definition of "Property" In The Crimes Act 1961 Include Electronically Stored Data? The Computer Says "No."" (LLB (Hons) Dissertation, University of Otago, 2015)

Kerr, Orrin "Cybercrime's Scope: Interpreting 'Access' and 'Authorisation' In Computer Misuse Statutes" (2003) 78(5) NYULR 1596

Kerr, Orrin "Norms of Computer Trespass" (2016) 116 Colum L Rev 1143

Kerr, Orrin "Vagueness Challenges to the Computer Fraud and Abuse Act" (2010) 94 Minn L Rev 1561

Lastowka, F. Gregory and Huntert, Dan "Virtual Crimes" (2005) 49 NYL Sch L Rev 293

Lessig, Lawrence "The Law of the Horse: What Cyberlaw Might Teach" (1999) 113 Harv L Rev 501

Moon, Ken "Intangibles as property and goods" (2009) 5 NZLJ 228

Richards, Jason "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security" (2009) 18 International Affairs Review 1

Trenwith, Anthony "A Patch On The System? E-Crime and the Crimes Amendment Act 2003" (2004) 10 Auckland University L Rev 90

von Hirsch, Andrew and Jareborg, Nils "Gauging Criminal Harms: A Living Standard Analysis" (1991) 11 Oxford J Legal Stud 1

Williams, Glanville "The Definition of a Crime" (1955) 1 CLP 1

G Government, Parliamentary, and Law Commission Materials

1 New Zealand

For the Crimes Amendment Bill 1989:

First Reading: (2 May 1989) 497 NZPD 10425

For the Crimes Amendment Bill 1999:

First Reading: (7 Sept 1999) 580 NZPD xv

Second Reading: (5 October 1999) 580 NZPD 19732

Consideration of the Report of the Select Committee Part 1: (12 June 2003) 609 NZPD 6238

Consideration of the Report of the Select Committee Part 2: (17 June 2003) 609 NZPD 6324

Third Reading: (1 July 2003) 609 NZPD 7082

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

Department of the Prime Minister and Cabinet *National Plan to Address Cybercrime 2015* (December 2015)

Law Commission *Computer Misuse* (NZLC R54, 1999)

Law Commission *Electronic Commerce Chapter One* (NZLC R50, 1998)

Law Commission *Privacy Concepts and Issues: Review of the Law of Privacy Stage 1* (NZLC SP19, 2008)

2 International

Cabinet Office of the United Kingdom *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world* (London, 2011)

Department of Prime Minster and Cabinet *Australia's Cyber Security Strategy: Enabling innovation, growth & prosperity* (Canberra, 2016)

Executive Office of the President of the United States, "The Comprehensive National Cybersecurity Initiative" WhiteHouse.gov (Washington D.C., 2008)

Royal Canadian Mounted Police *Royal Canadian Mounted Police Cybercrime Strategy* (Ottawa, 2015)

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

United Kingdom Law Commission *Working Paper No. 110: Computer Misuse* (London, 1988)

United Kingdom Law Commission, *Report 186: Computer Misuse* (London, 1989)

H Other Texts

Marshall Jarrett, H., Bailie, Michael, Hagen, Ed, and Eltringham, Scott *Prosecuting Computer Crimes* (2nd ed., United States Department of Justice, Washington D.C., 2010)

Ablon, Lillian, Libicki, Martin C., Golay, Andrea A. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar* (RAND Corporation, California, 2014)

Office of Technology Assessment *Selected Electronic Funds Transfer Issues: Privacy, Security, and Equity* (Diane Publishing, Pennsylvania, 1982)

New Zealand Institute of Directors *Cyber-Risk Practice Guide* (New Zealand Institute of Directors, Wellington, 2016)

I Interviews, Presentations, and Speeches

Bruce Slane, Privacy Commissioner "Privacy protection: A Key To Electronic Commerce" (New Zealand Law Conference, Rotorua, 9 April 1999)

Interview with 'Spasrat' (identity obscured), computer hacker (Paul Holmes, "Holmes", 20 November 1998)

Jennifer Granick, Director of Civil Liberties at the Stanford Center for Internet and Society ("Innovation or Exploitation? The Limits of Computer Trespass Law", Stanford Law School, Stanford, California, February 19, 2013)

J Online

Australian Institute of Criminology "High tech crime brief no. 5" AIC (January 2005) <http://www.aic.gov.au/publications/current%20series/htcb/1-20/htcb005.html>

Barton, Chris "Anti-hacking policy masks hidden agenda" New Zealand Herald Online (5 March 2003) <http://www.nzherald.co.nz/technology/news/article.cfm?c_id=5&objectid=3198788>

Computer Ethics Institute "The Ten Commandments of Computer Ethics" (1 September 2011) CPSR <http://cpsr.org/issues/ethics/cei/>

Crown Prosecution Services (UK) "Computer Misuse Act 1990" CPS <http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/>

Dodd, Vikram "Police to hire law firms to tackle cyber criminals in radical pilot project" (14 August 2016) The Guardian Online <https://www.theguardian.com/uk-news/2016/aug/14/police-to-hire-law-firms-to-tackle-cyber-criminals-in-radical-pilot-project>

Doherty, Mike "SCI 4192 Report 1: Problematic Computer Crime Law In Canada" (October 31 2013) HashBang <https://hashbang.ca/wp-content/uploads/2013/11/report1.pdf>

Eden, John “Man admits hacking ex's emails” (14 January 2015) Stuff.co.nz <http://www.stuff.co.nz/national/crime/64925409/man-admits-hacking-exs-emails>

Geddis, Prof. Andrew “Dixon v R: An easy case that raises hard questions” (20 October 2015) Pundit.co.nz <http://pundit.co.nz/content/dixon-v-r-an-easy-case-that-raises-hard-questions>

Goldman, Eric “The Third Wave of Internet Exceptionalism” (11 March 2009) Technology & Marketing Law Blog <http://blog.ericgoldman.org/archives/2009/03/the_third_wave.htm>

Harvey, Judge David “The Crimes Amendment Act 2003 and the Government Communications Security Act 2003 – An Interrelated History” (25 August 2013) The IT Countrey Justice <https://theitcountreyjustice.wordpress.com/2013/08/25/the-crimes-amendment-act-2003-and-the-government-communications-security-act-2003-an-interrelated-history/>

McCarthy, Kieren “'Aaron's Law' back on the table to bring sanity to US hacking laws” (23 April 2015) The Register <http://www.theregister.co.uk/2015/04/23/congress_reintroduces_aarons_law/>

McCarthy, Ross “FBI website hacker Charlton Floate, 19, facing jail for cyber attacks” (19 August 2015) Birmingham Mail Online <http://www.birminghammail.co.uk/news/midlands-news/fbi-website-hacker-charlton-floate-9887386>

Mueller, Bianca “Criminal liability for mobile phone spying in NZ” (31 January 2014) LawTalk – New Zealand Law Society <https://www.lawsociety.org.nz/lawtalk/lawtalk-archives/issue-834/criminal-liability-for-mobile-phone-spying-in-nz>

Oliver. John “Encryption: Last Week Tonight with John Oliver” (13 March 2016) YouTube <https://youtu.be/zsjZ2r9Ygzw?t=5m4s>

Turner, Michael “Computer Misuse Act 1990 cases” (2016) Computer Evidence <http://www.computerevidence.co.uk/Cases/CMA.htm>

Wearden, Graeme and Espine, Tom “UK law will criminalise IT pros, say experts” (19 May 2006) ZDNet <http://www.zdnet.com/article/uk-law-will-criminalise-it-pros-say-experts/>

“A former policeman accessed his ex-girlfriend's Facebook account illegally” (21 September 2016) Stuff.co.nz <http://www.stuff.co.nz/national/crime/84494407/a-former-policeman-accessed-his-exgirlfriends-facebook-account-illegally>

“Computer repair man's offending 'disturbing and sinister'” (26 March 2010) Stuff.co.nz <http://www.stuff.co.nz/national/crime/3511791/Computer-repair-mans-offending-disturbing-and-sinister>

“Definition of ‘computer’” Merriam-Webster Dictionary Online <http://www.merriam-webster.com/dictionary/computer>

“Marlborough man charged for hacking wife's Facebook account” (21 June 2016) Marlborough Express Online <http://ssl-www.stuff.co.nz/marlborough-express/news/81277346/Marlborough-man-charged-for-hacking-wifes-Facebook-account>

K Online – General Computer Crime Background Reading

Arthur, Charles “Naked celebrity hack: security experts focus on iCloud backup theory” (1 September 2014) The Guardian Online <https://www.theguardian.com/technology/2014/sep/01/naked-celebrity-hack-icloud-backup-jennifer-lawrence>

Brandon, John “The FBI and Apple encryption battle is over, now the true debate begins” (28 March 2016) Computerworld <http://www.computerworld.com/article/3048547/apple-ios/the-fbi-and-apple-encryption-battle-is-over-now-the-true-debate-begins.html>

Bugayenko, Yegor “Five Principles of Bug Tracking” (24 November 2014) <http://www.yegor256.com/2014/11/24/principles-of-bug-tracking.html>

Encyclopaedia Britannica “Procrustes” Encyclopaedia Britannica Online <https://www.britannica.com/topic/Procrustes>

Evangeli, Nina “Going through someone else’s phone is never OK” The Tab <http://thetab.com/2016/03/07/going-someone-elses-phone-never-ok-78499>

Fahmida Rashid “Cyber criminals cash out using PowerShell, other legitimate tools” (8 February 2016) InfoWorld <http://www.infoworld.com/article/3030689/security/cyber-criminals-cash-out-using-powershell-other-legitimate-tools.html>

Fiegerman, Seth “Yahoo says 500 million accounts stolen” (23 September 2016) CNN Money http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/>

Field, Michael “Telstra offshoot hires teen hacker 'Akill'” (24 March 2009) Sydney Morning Herald Online <http://www.smh.com.au/national/telstra-offshoot-hires-teen-hacker-akill-20090323-97yn.html>

Fogarty, Kevin “Tech predictions gone wrong” (22 October 2012) ComputerWorld <http://www.computerworld.com/article/2492617/it-management/tech-predictions-gone-wrong.html>

Greenberg, Andy “Hackers Remotely Kill a Jeep on the Highway—With Me in It” (21 July 2015) Wired.com <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>

Honan, Matt “What Not to Do with Someone Else's Phone” (6 October 2011) Gizmodo <http://gizmodo.com/5810782/what-not-to-do-with-someone-elses-phone>

Lamont, Tom “Life after the Ashley Madison affair” The Guardian (28 February 2016) <https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked>

Lee, Timothy “The Sony hack: how it happened, who is responsible, and what we've learned” (17 December 2014) Vox <http://www.vox.com/2014/12/14/7387945/sony-hack-explained>

Leyden, John “'80s hacker turned journo, IT crime ace Steve Gold logs off” (13 January 2015) The Register http://www.theregister.co.uk/2015/01/13/steve_gold_obit/>

Lee, Francesca “Hacking of Facebook often easy to do” (7 April 2012) The Press Online http://www.stuff.co.nz/the-press/news/6706956/Hacking-of-Facebook-often-easy-to-do>

MacLeod, Scott “Hacker tapped into accounts, police claim” (30 June 2000) Stuff.co.nz <http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=118209>

Newman, Lily “Security News This Week: The DNC Hack Was Worse Than We Thought” (13 August 2016) Wired.com <https://www.wired.com/2016/08/security-news-week-dnc-hack-worse-thought/>

Quinn, Ben and Arthur, Charles “PlayStation Network hackers access data of 77 million users” (26 April 2011) The Guardian <https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data>

Shuttleworth, Kate “MSD shuts WINZ kiosks after lax security exposed” (15 October 2012) New Zealand Herald Online <http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10840563>

Slater, Joanna “After Bangladesh: How a massive hack shook the banking world” (12 June 2016) The Globe and Mail <http://www.theglobeandmail.com/report-on-business/international-business/cybertheft-of-bangladeshs-central-bank-threatens-global-bank-system/article30408324/>

Tait, Morgan “NZ in sophisticated cyber crime attack” (April 12 2016) New Zealand Herald Online <http://nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11621227>

Taylor, Andy “The Internet of Things, cyber-security and the role of the CIO” (20 September 2016) SC Magazine UK <http://www.scmagazineuk.com/the-internet-of-things-cyber-security-and-the-role-of-the-cio/article/521127/>

Vance, Andrea “Fears cyberbullying law will criminalise children” (24 March 2015) Stuff.co.nz <http://www.stuff.co.nz/technology/digital-living/67487381/fears-cyberbullying-law-will-criminalise-children>

Veldhuijzen van Zanten, Boris “The very first recorded computer bug” (19 September 2013) TheNextWeb <http://thenextweb.com/shareables/2013/09/18/the-very-first-computer-bug/>

Winter, Chloe “Cyber crime continues to rise” (18 May 2015) Stuff.co.nz <http://www.stuff.co.nz/technology/digital-living/68636916/cyber-crime-continues-to-rise>

Zetter, Kim “An Unprecedented Look at Stuxnet, the World’s First Digital Weapon” (3 November 2014) Wired.com <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>

“Census: Australian Bureau of Statistics says website attacked by overseas hackers” (10 August 2016) ABC News <http://www.abc.net.au/news/2016-08-10/australian-bureau-of-statistics-says-census-website-hacked/7712216>

“Cyber crime – the hidden epidemic hurting our businesses” (2 May 2016) New Zealand Herald Online <http://www.nzherald.co.nz/sponsored-stories/news/article.cfm?c_id=1503708&objectid=11630920>

“FBI Director: Hacking Will Replace Terrorism As The Nation's Top Worry” (2 March 2012) Business Insider Australia <www.businessinsider.com.au/robert-mueller-fbi-hacking-terrorism-2012-3?r=US&IR=T>

“The Heartbleed Bug” (2014) Codenomicon <http://heartbleed.com/>