JUDITH JEFFERSON

CYBERPORN: INVESTIGATORY AND PROSECUTORIAL ISSUES RELATING TO CHILD PORNOGRPAHY IN THE NEW ZEALAND CONTEXT

LLM RESEARCH PAPER
CYBERSPACE LAW (LAWS 520)

LAW FACULTY
VICTORIA UNIVERSITY OF WELLINGTON

2001

CONTENTS

ABSTRACT

The Films, Videos, and Publications Classification Act 1993 was enacted prior to the Internet-revolution. As such, the Act responded to the challenges of objectionable material in physical form. This paper examines, from a law enforcement perspective, the responsiveness of the Act to child pornography in the Internet-age. The exploration of the resulting issues is influenced by the prime objective of the Act in respect of child pornography: to ban child pornography from New Zealand.

While this paper does not intend to reach definitive conclusions, it is clear that New Zealand needs to address the realities of a borderless community. Action must be taken to address the significant investigatory weaknesses and, to a lesser extent, prosecutorial challenges caused the Act's pre-Internet origins.

Any attempt to achieve an effective ban on Internet child pornography will require a combination of technological and legislative responses. However, individual State law enforcement agencies cannot successfully confront the issue in isolation. An international multiagency response is required to effectively deal with child pornography on the Internet.

The text of this paper (excluding contents page, footnotes, bibliography and annexures) comprises approximately 7,500 words.

I INTRODUCTION

The year, 1993: the eve of the Internet revolution. New Zealand had the luxury of isolation: borders that were physical, not just lines on a map. That isolation gave a sense of remoteness from "overseas" problems like child pornography. Comfort was taken in the fact that child pornography, at that time, could only get into New Zealand in physical form: books, videos, and films. The comments of the 1989 Committee of Inquiry into Pornography reveals the feelings of security that isolation brought:[1]

> While it is clear that child pornography is available in New Zealand, little is known about its extent. . . . We assume that some child pornography that is commercially produced, especially in the United States and Europe, is brought into the country in person or by mail, by those interested in obtaining this material. However, Customs has not seized any such material in the last four or five years.

Parliament's response to the outside threat of child pornography was to pass the Films, Videos, and Publications Act 1993 ("FVPCA").

When the Films, Videos, and Publications Classification Bill was introduced to the House a greater understanding of the issues surrounding child pornography within New Zealand was starting to develop.[2] However, only one Member, the Hon G Lee, recognised

---

[1] Committee of Inquiry into Pornography *Pornography: Report of the Ministerial Committee of Inquiry into Pornography* (Department of Justice, Wellington, 1989) 43.

[2] See the comments of Hon TWM Tirikatene-Sullivan (2 December 1992) 532 NZPD 12772 with regard to the growing number of seizures of pornographic videotapes, at that time the matter was before the House.

that the format of pornography delivery may change.[3] He called it "high technology pornography". He envisaged "bulletin boards" and "video phones" being the means of delivery. At that time no one foresaw the Internet and the window of opportunity it brought to all, including those who wished to access child pornography. Today though, that realisation is truly upon New Zealand and the rest of the international community.[4] Interpol has categorised present reality in this manner:[5]

> The growth of information technology has transformed the production of child pornography into a sophisticated, world-wide "cottage" industry: this means that technology has made it possible to produce and distribute pornographic material at home. Anyone with access to a personal computer and a modem can connect up to commercial on-line services and to the Internet, this remarkable computer network connecting millions of people all over the world.
>
> In fact, today and in the future, the Internet is well on its way to becoming the most significant factor in child sexual exploitation, and the principal means for exchanging child pornography. It defies comparison with all other means communication, both traditional and modern.

The purpose of this research is to examine the impact of the Internet on the enforcement of the FVPCA.[6] The paper aims to examine the consequences for FVPCA investigations and prosecutions where offending relating to child pornography is facilitated by online

---

[3] Hon G Lee (2 December 1992) 532 NZPD 12767.

[4] If evidence is required, see the papers presented to the Combating Child Pornography on the Internet Conference held in Vienna on 29 September – 1 October 1999. The papers are available from <http://www.stop-childpornog.at>.

[5] Agnès Fournier de Saint Maur "The Sexual Abuse of Children via the Internet: a New Challenge for Interpol" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999) <http://www.stop-childpornog.at/ab_maur.asp> (last accessed 3 May 2001).

[6] This paper concentrates on enforcement of the Films. Videos, and Publications Classification Act 1993 ("FVPCA") from the perspective of the New Zealand Police. While enforcement officers from the Department of Internal Affairs have the major role in respect of enforcing the FVPCA, this area is a growing portion of Police work and closely related to the investigation of paedophilic activities.

means. This paper serves more to identify issues and suggest options for addressing those issues rather than to reach definitive conclusions.

II CHILD PORNOGRAPHY - A WORKING DEFINITION

To facilitate clarity, it is appropriate that what is meant by "child pornography" is generally understood. While it will become clear that for the purposes of the operation of the FVPCA the term "child pornography" is not critical, perceptions of pornography can be very subjective. Pornography comes from the Greek roots "porne" and "graphos". Feminist writer Andrea Dworkin has rendered the literal translation of those terms as "the graphic portrayal of woman as whores".[7] That particular definition conveys the inherent degradation present in such material. Interpol has adopted the following definition specific to child pornography:[8]

> Child pornography is created as a consequence of sexual exploitation or abuse of a child. It can be defined as any means of depicting or promoting the sexual exploitation of a child, including written or audio material, which focuses on the child's sexual behaviour or genitals.

That definition provides an adequate working definition of "child pornography" for the purposes of this paper.

---

[7] Andrea Dworkin "Pornography and male supremacy" *Letters from a War Zone* (Secker and Warburg, London, 1988) 230.

[8] Agnès Fournier de Saint Maur "The Sexual Abuse of Children via the Internet: a New Challenge for Interpol" (Combating Child Pornography on the Internet,

III THE FILMS, VIDEOS, AND PUBLICATIONS CLASSIFICATION ACT 1993

A Purpose and Policy

The FVPCA provided New Zealand's first unified classification and enforcement regime for all types of publications.[9, 10] It was heralded as a means of providing an integrated approach, a "clear, coherent, and purposeful [piece of] legislation ... to rationalise the approach to classification of visual and printed matter, to revise and reform the criteria of classification, and to facilitate public access to the classification system".[11]

In addition to unifying censorship processes, the FVPCA had a specific purpose in respect of child pornography:[12]

> [O]ne category of material is marked for prohibition on its own terms. The Government has decide that all forms of child pornography will be banned outright ... The Government believes that it is not acceptable for this type of material to be available, so the opportunity for abusers of any type to have the use of this pornography to excite themselves, or to condition their victims, will no longer be available.

Vienna, 29 September – 1 October 1999) <http://www.stop-childpornog.at/ab_maur.asp> (last accessed 3 May 2001).

[9] The FVPCA came into full force on 1 October 1994: Films, Videos, and Publications Classification Act Commencement Order 1994.

[10] The only matters to fall outside the provisions of the legislation are matters covered by the Broadcasting Standards Authority under the Broadcasting Act 1989.

[11] Hon J Shipley (2 December 1992) 532 NZPD 12758.

[12] Hon J Shipley (2 December 1992) 532 NZPD 12759-12760.

Thus, Parliament specifically acknowledged where the real harm in child pornography lies: the use of child pornography by paedophiles both for their own pleasure and, more ominously, as a means to make their victims more receptive to their paedophilic advances. As Interpol has stated "pornography is used by child abusers as a mean [sic] of desensitising children in order 'to lower their inhibitions'."[13] That process may take years and relies upon progressive exposure to material of escalating sexual content. The process, if successful, really amounts to a reconditioning of the child or young person away from the generally accepted social prohibition on sexual activity between children or young persons and adults.

In acknowledging the role pornography has in conditioning a victim, Parliament recognised the potential for harm created by the mere availability of such material: it puts the most vulnerable group in our society at greater risk of victimisation.

---

[13] Agnès Fournier de Saint Maur "The Sexual Abuse of Children via the Internet: a New Challenge for Interpol" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999) <http://www.stop-childpornog.at/ab_maur.asp> (last accessed 3 May 2001).

B Key Definitions

1 "Publication"

As a result of the unified classification approach, and its corollary need to cover a diverse range of media, "publication" was given a broad meaning in section 2.[14] "Publication" means:

> (a) Any film, book, sound recording, picture, newspaper, photograph, photographic negative, photographic plate, or photographic slide:
> (b) Any print or writing:
> (c) Any paper or other thing—
> (i) That has printed or impressed upon it, or otherwise shown upon it, any word, statement, sign, or representation; or
> (ii) On which is recorded or stored any information that, by the use of any computer or other electronic device, is capable of being reproduced or shown as any word, statement, sign, or representation.

Section 2(c)(ii) attempts to provide a technology-neutral definition. All that subparagraph requires for a publication is a means of storing information which, by application of technology, results in comprehensible representations. It is clearly broad enough to encompass data present in a computer system or network, including the Internet.

2 "Objectionable material"

(a) Legislative provisions

The other key concept that the FVPCA turns upon is the concept of objectionability.

The general definition of what is objectionable is contained in section 3(1):

> For the purposes of this Act, a publication is objectionable if it describes, depicts, expresses, or otherwise deals with matters such as sex, horror, crime, cruelty, or violence in such a manner that the availability of the publication is likely to be injurious to the public good.

According to *Moonen v Film and Literature Board of Review* (1999) 17 CRNZ 159 that "general test" is given effect by the subsequent subsections.[15] A publication will, therefore, be "objectionable" if it is:

(a) Classified as objectionable by the Office of the Censor; or

(b) Deemed objectionable by s 3(2) FVPCA.[16]

Section 3(2) provides:

> A publication shall be deemed to be objectionable for the purposes of this Act if the publication promotes or supports, or tends to promote or support,—
> (a) The exploitation of children, or young persons, or both, for sexual purposes; or
> (b) The use of violence or coercion to compel any person to participate in, or submit to, sexual conduct; or
> (c) Sexual conduct with or upon the body of a dead person; or
> (d) The use of urine or excrement in association with degrading or dehumanising conduct or sexual conduct; or
> (e) Bestiality; or
> (f) Acts of torture or the infliction of extreme violence or extreme cruelty.

It should be noted that all the acts specified in subsection 2, with the exception of paragraph (d), involve criminal conduct.[17]

---

[14] See the Appendix to this paper for all legislative provisions of substantive importance to this paper.
[15] *Moonen v Film and Literature Board of Review* (1999) 17 CRNZ 159, para 4.
[16] *Moonen v Film and Literature Board of Review* (1999) 17 CRNZ 159, para 5.

It is material that falls under section 3(2)(a) FVPCA that is of concern in this paper: publications that promote, support, or tend to promote or support, the exploitation of children, or young persons, or both for sexual purposes.

(b) Effect of the *Moonen* decision

By dint of that provision child pornography is, or at least was intended to be,[18] automatically objectionable and therefore banned.[19] The intention of the provision was clear until December 1999 when the Court of Appeal delivered its decision in *Moonen v Film and Literature Board of Review.*[20] That case introduced section 14 New Zealand Bill of Rights Act 1990 (freedom of expression) considerations into the process of deciding whether a publication "promotes or supports, or tends to promote or support" the prohibited activity. *Moonen* held that those words required more than mere depiction.[21] The effect of the publication must be to advocate or encourage the exploitation of children or young persons for sexual purposes.

---

[17] See Part VII Crimes Act 1961. In particular, see: ss 127-129A, ss 131-135, ss 139-141 (sexual assaults and sexual conduct with minors provisions), ss 143 (bestiality), and s 150 (misconduct in respect of human remains).

[18] "The Government has decided that all forms of child pornography will be banned outright." Hon J Shipley's comments in the introduction speech for the Films, Videos, and Publications Classification Bill: Hon J Shipley (2 December 1992) 532 NZPD 12759.

[19] Presently the Department of Internal Affairs continues to hold that position in their advice to their Minister: Department of Internal Affairs *Briefing to the Minister of Internal Affairs: November 2000* (Wellington, 2000) part 8, 3.

[20] *Moonen v Film and Literature Board of Review* (1999) 17 CRNZ 159.

In the prior leading case, *News Media Ltd v Film and Literature Board of Review* (1997) 4 HRNZ 410 the High Court held that section 3 is inconsistent with freedom of expression rights and, therefore, they do not constrain the application of section 3.[22] Currently, however, there is a level of uncertainty as to what will and will not be deemed objectionable. Can any material be automatically objectionable? In light of the *Moonen* decision, the answer is probably no.

Reaction to the *Moonen* decision lead to the introduction of the Films, Videos, and Publications Classification (Prohibition of Child Pornography) Amendment Bill on 2 August 2000. The stated aim of that Bill is to reverse the effect of the *Moonen* decision, and return the section 3(2) deeming provisions to the status of an automatic prohibition.[23] The Government Administration Select Committee has been charged, as a result of the Bill, with inquiring into the workings of the FVPCA. The Terms of Reference of the Inquiry of the Government Administration Committee into the Operation of the Films, Videos, and Publications Classification Act 1993 and Related Issues include inquiring into:[24]

---

[21] *Moonen v Film and Literature Board of Review* (1999) 17 CRNZ 159, para 29.
[22] *News Media Ltd v Film and Literature Board of Review* (1997) 4 HRNZ 410, 420.
[23] See the speech of the Hon Anne Tolley on (16 August 2000) 586 NZPD 4931.
[24] Government Administration Select Committee "The Terms of Reference of the Inquiry of the Government Administration Committee into the Operation of the Films, Videos, and Publications Classification Act 1993 and Related Issues" (Wellington, 2001) <http://www.clerk.parliament.govt.nz/publications/GAtor.htm> (last accessed 13 June 2001).

(a) "The definition of 'objectionable', ... to determine whether the Court of Appeal's narrow interpretation [in *Moonen*] adequately carr[ies] out the intent of the Act"; and

(b) "Whether ... the Bill of Rights Act 1990 [sic] should apply to all matters prescribed in [section 3(2)] of the Act or whether ... publications that promote the matters in that section [should be] 'objectionable' [notwithstanding the 1990 Act]".

To that end, the Select Committee received submissions on the issue until 4 May 2001. The matter remains before the Committee.

3 "Child" or "young person"

It will be noted that what constitutes a child or young person for the purposes of the FVPCA is not defined.[25] However, for the purpose of the FVPCA the actual age of the individual portrayed in the publication is irrelevant.

News Media demonstrates this point.[26] In that case the *New Truth* newspaper published classified advertisements for sexual

---

[25] As a general guide the definitions provided by section 2 Children, Young Persons, and their Families Act 1989 are helpful. A "child" is a girl or boy under 14 and a "young person" is a boy or girl over 14 but under 17.

[26] *News Media Ltd v Film and Literature Board of Review* (1997) 4 HRNZ 410.

services. Some of the advertisements included references to schoolchildren.[27] The High Court stated:[28]

> It is possible that the asserted "school boys" or "school girls" are somewhat older; but titillation of that character can create an atmosphere in which the minds of some later will turn to the real thing.

Thus, establishing age is not a necessary element in establishing objectionability under section 3(2)(a).

Nor, by the same logic, is it necessary to establish that the person depicted in images is a real individual. The Internet provides the ability to alter pictures and create pseudo and morphed children. Overseas, there are some jurisdictions in which digitally altered or produced images do not fall within the definition of the prohibited material because of the wording of the offence.[29] *Moonen*, however, makes it clear the key is the publication's effect, not merely the depiction itself.[30]

C Offences

For the purposes of this paper, consideration of offences relating to objection material will be limited to sections 123, 124, and 131. Section 127 also deals with objectionable material, in respect to

---

[27] For example: "Naughty School Girls" was the title for a peep show advertisement.
[28] *News Media Ltd v Film and Literature Board of Review* (1997) 4 HRNZ 410, 420
[29] Ulrich Sieber *Criminal Law Provisions against Child Pornography: A Legal Comparative Study for the Creation of Worldwide Minimum Standards* (German Federal Ministry of Justice, Bonn, 1999).

exhibiting or displaying objectionable material to an individual under 18 years of age. However, the focus of this paper is on the implications of the Internet's facilitation of transactional and possessory activities, not end-use results in and of themselves.

1 Generation and dissemination offences

Sections 123 and 124 can be readily classified as generation and dissemination offences. Those sections deal with the activities of creating and distributing, or offering for distribution, publications which fall foul of section 3 FVPCA. The prohibited activities involve making, copying, supplying, and distributing objectionable publications.

In respect to these generation and dissemination activities, there are two types of offences: strict liability and mens rea offences.

(a) Strict liability offences

The strict liability offences are set out in section 123. The imposition of strict liability is achieved through subsection 3, which provides that absence of knowledge, or reasonable cause to believe that the material was objectionable is no defence.[31]

---

[30] *Moonen v Film and Literature Board of Review* (1999) 17 CRNZ 159, para 29.

[31] There has been no New Zealand examination of whether, not withstanding that provision, there could be a defence of absence of fault. For an examination of the defence of absence of fault see *Mackenzie v Civil Aviation Department* (1983) 1 CRNZ 38. However, given the purpose of the legislation was to ban child pornography in New Zealand it would appear that subsection 3 is aimed at effecting that ban. In light of *Millar v Ministry of Transport* (1986) 2 CRNZ 216 the legislative purpose is highly suggestive of an absolute offence classification, as an absence of fault defence would rapidly undermine ban on child pornography.

(i) Impact for ISPs

Section 123(1)(b) has significant import for Internet service providers ("ISPs"). It provides that it is an offence to copy an objectionable publication for the purpose of distribution. "Distribute" is defined in section 122 as meaning "to deliver, to give, or to offer". The very nature and purpose of ISP activities, delivering copies of pages called upon to the computer accessing a site, is caught by the concept of "distribution". When such potential for primary liability exists,[32] there is no need to examine concepts of ISP secondary liability.[33]

(ii) Non-commercial activity

Section 123(4) FVPCA provides that:

> Without limiting the generality of this section, a publication may be—
>
> (a) Supplied (within the meaning of that term in section 2 of this Act) for the purposes of paragraphs (b), (c), and (d) of subsection (1) of this section; or
>
> (b) Made available for the purposes of paragraph (e) of that subsection—
>
> not only in a physical form but also by means of the electronic transmission (whether by way of facsimile transmission, electronic mail, or other similar means of communication, other than by broadcasting) of the contents of the publication.

---

[32] While an ISP may not escape liability on the basis of absence of fault (if the strict liability categorisation is correct), another defence may be available. It is a defence to a charge of possession if the ISP is not aware that it possesses the material at all (independent of awareness of content). See *Julian v Green* (1989) 5 CRNZ 97, 98: "A person cannot possess something of which he [or she] is unaware". The factual circumstances of each particular case will be influential in any decision as to "awareness".

[33] Of course, whether prosecutions against ISP would be appropriate from a practical co-operation perspective, is another question.

Thus, there is no question that electronic delivery methods are covered where the material is being sold, hired, or offered for sale or hire within the frame work of the particular provisions.

While prefaced "without limiting the generality of this section", this subsection brings into clear focus the question of whether monetary consideration is a necessary element of a transaction involving child pornography before a FVPCA offence will be established.[34] This is of particular import for policing paedophile groups like the Wonderland Club. That group had an entry "fee" of 10,000 child pornography images. Its membership was about mutual "appreciation" of child pornography, not commercial gain. Publications in such circumstances cannot, in any normal sense of the words, be said to be sold, hired, or offered for sale or hire. Thus, any Wonderland Club-type transaction would not amount to "supplying".[35]

However, a further question arises. Does section 123(4) have any import in respect to electronic distribution offences under section 123(1)(b) FVPCA where no consideration is given or received? While there is no precedent on this point, the preliminary words of section 123(4) appear to permit the application of section 123 to the electronic delivery of objectionable publications where no consideration is exchanged. The perceived need for

---

[34]"Paedophiles jailed for porn ring" (13 February 2001) *BBC News Online* United Kingdom <http://news.bbc.co.uk/hi/english/uk/newsid_1168000/1168112.stm> (last accessed on 20 May 2001).

section 123(4) may have been based upon a concern as to whether there could be online contract formation. This makes some sense given that the Act was, after all, prepared while debate still raged as to whether offer and acceptance by electronic means was possible.[36]

(b) Mens rea offences

Section 124 provides that all the acts punishable under section 123(1) are subject to a higher penalty where they are committed with knowledge or reasonable cause to believe that the material is objectionable. In the case of an individual, the penalty is one year's imprisonment or a $20,000 fine; a corporation is subject to a $50,000 fine. Those penalties compare with fines of $5,000 and $15,000, respectively, for the equivalent strict liability offences.

Given that paedophiles very rationale for dealing with objectionable material is that it does depict the exploitation of children for sexual purposes, theoretically intention should be easily established. However, the key is providing probative evidence without prejudicing the defendant. While search history data may be valuable in demonstrating intention of the computer user, establishing the identity of the computer user at the time relevant searches were

---

[35] That applies to physical transactions, as well, where there is no commercial transaction.

[36] That debate has yet to be permanently settled. "Today, our legal system is riddled with rules and requirements that are based on the primacy of paper. The growth of the Internet and electronic communications has called into question the legitimacy of those paper-based rules. Indeed, these requirements are often viewed as barriers to electronic commerce, both domestically and internationally." Amelia H Boss "Tearing Down Paper Barriers" (14 February 2000) *Legal Times* United States <http://www5.law.com/dc-shl/display.cfm?id=2732> (last visited 18 June 2001).

conducted provides another difficulty. Conclusively establishing that the defendant is the person who conducted the relevant searches will depend on inculpatory statements made in respect of restrictions on access to and use of the computer in question.

2 Possession

Section 131 provides for a strict liability offence (subsection 3) for possession of objectionable material without lawful authority or excuse.[37] The penalty for a corporation possessing objectionable material is a $5,000 fine. An individual faces a fine of $2,000.

Again, ISPs face the sceptre of criminal liability without having knowledge, or even reasonable cause to suspect, that the material on their servers is objectionable.

D Search and Seizure

Given the predominance of monetary penalties for offences under the FVPCA, specific search and seizure powers were required. Generally, section 198 Summary Proceedings Act 1957 provides sufficient search powers for offences. However, it requires that the suspected offence be one carrying a penalty of imprisonment. Thus, without specific provisions the FVPCA would have been ineffectual in respect of locating evidence and seizing objectionable material.

1 FVPCA warrant

Under the FVPCA objectionable material can be searched for and seized under a section 109 warrant. Such a warrant can only be granted by a judicial officer.[38] He or she must have reasonable grounds to believe that there is in or on any place or thing:[39]

(a) An objectionable publication that is being kept for the purposes of committing an offence under sections 123, 124,[40] 127, and 129;[41]

(b) Any evidence of such offence; or

(c) Any thing intended to be used for the purpose of committing such an offence.

The application has to be made by a Police Officer[42] on oath, in writing, setting out the grounds for the application to enable the judicial officer to reasonably conclude that one of the relevant limbs of section 109(1) has been established.

It is imperative to recognise that by limiting the offence provisions to sections 123, 124, 127, and 129, there is no power to

---

[37] Subsections 3 and 4 provide certain classes of persons with authority or excuse to possess objectionable material. The aim of these provisions will enable the effective disposal of proceedings under the FVPCA.

[38] Either a District Court Judge, Justice of the Peace, Community Magistrate, or Registrar.

[39] Section 109(1)(a), (b), and (c) FVPCA.

[40] The making or dissemination offences, with and without mens rea.

[41] The display of objection material offences.

[42] Or an Inspector.

obtain a search warrant for an offence of mere possession of objectionable material under section 131 FVPCA.

2 Seizure without warrant

However, from a policing perspective,[43] it is more common for objectionable material to be seized during the execution of lawful duty. Under section 108, upon discovering a publication that an Officer believes, on reasonable grounds, to be objectionable, he or she may seize the item without requiring further authority. Section 108 provides the only authority to seize objectionable material that is merely being possessed (section 131), as opposed to generated or disseminated (sections 123 or 124).

Where electronic material is found and seized under section 108 there may be reasonable grounds to justify applying for and obtaining a section 109 warrant to search for further material or seize equipment.[44]

---

[43] Given the nature of Police work including resourcing and prioritisation of offence investigations.

[44] For example, where computer disks are located which suggest by some means, most usually labelling, that they contain objectionable material, if there is also a computer present with an internet connection, it may give rise to the belief that an offence under section 123(1)(b) (a copying offence) has or is intended to be committed via that computer. A search warrant in those circumstances may be obtained to seize the computer or, alternatively, the data by cloning the computer.

E Other Practical Matters

1 Authority to prosecute

Once material has been seized and been determined to be within section 3(2), an authorisation to prosecute must be obtained.

The power to consent to prosecution has been delegated by the Attorney-General to the Commissioner of Police under section 144. The Commissioner in turn has delegated that power to the District Commanders (who hold the rank of Superintendent). That delegation was achieved by written authority dated 28 October 1997 pursuant to section 145.[45]

---

[45] Before a District Commander can authorise a prosecution, legal advice must be given as to "objectionability". In addition, the District Commander has to formulate his or her own conclusion that the material is objectionable.

As a result of *Moonen v Film and Literature Board of Review* (1999) 17 CRNZ 159 both the Legal Adviser (in giving advise on whether the material falls foul of section 3(2)(a)) and the District Commander (in reaching a conclusion as to objectionability), need to consider New Zealand Bill of Rights Act 1990 considerations. Thus, every decision to charge a person with an offence under the FVPCA, even that of simple possession, will have to first consider whether it is demonstrably justified in a free and democratic society to view the publication as promoting or supporting, or tending to promote or support, the sexual exploitation of children and young people. The fact that a publication provides "sexual titillation" based upon the exploitation of children and young persons appears to provide no justification to conclude that it should be deemed objectionable. There must be something more than mere depiction. In addition, the reasons for finding that the depiction has the prohibited effect must be clearly spelt out by both the Legal Adviser providing the advice and the District Manager.

Moonen raises the reality that every decision to prosecute could be subject to challenge for breach of section 14 New Zealand Bill of Rights Act, if the decision maker fails to adequately articulate why he or she decided that the material promoted or supported, or tended to promoted or support, the sexual exploitation of children or young persons.

2 *Laying of Charges*

Once charges have been authorised, they may be laid in the District Court's summary jurisdiction: section 142 FVPCA. Under section 143 Police have two years to lay the charge.

IV THE IMPACT OF THE INTERNET

A Introduction

There can be no question that the Internet has given the opportunity to access a vast array of child pornography material that was not physically available in New Zealand before its advent. This is demonstrated by contrasting the absolute minimal seizures described by the Committee of Inquiry into Pornography with Max Taylor's research observations about material available globally.[46] As Professor Taylor notes, though, asking how much more objectionable material is available to Internet users may not be the sensible question. He suggests that the "more sensible and more frightening question to ask . . . is how many children are involved."[47]

---

[46] Compare Committee of Inquiry into Pornography *Pornography: Report of the Ministerial Committee of Inquiry into Pornography* (Department of Justice, Wellington, 1989) 43 and Max Taylor "The Nature and Dimensions of Child Pornography on the Internet" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999) <http://www.stop-childpornog.at/pa_taylor.html> (last accessed 3 May 2001).

[47] Professor Taylor concludes that in a 50,000 picture sample (all of which were downloaded from the Internet), there are 2,000 (different) boys and girls shown in explicit sexual situations and another 2,000 positioned in erotic nude poses. Only

B Feature Advantageous to Child Pornographers

Cyberspace has a greater effect than merely allowing access to greater amounts and diversity of material. It facilitates a number of features beneficial to users of child pornography:

(a) A generally free source of material without physical boundaries to restrain access.

(b) A near instantaneous means of satisfying the desire for more material.[48] That ability to access new and exciting material as one desires without practical barriers to require the controlling of that desire may lead to habituation. Habituation in return may lead to a greater propensity to attempt real-world offending against children:[49]

> A recent quotation from a posting to a paedophile Bulletin Board illustrates this process from the user's perspective "... With this hobby [referring to paedophilia] we get bored after a while with the usual and we risk a bit to get new stuff or actual

---

15% of the sexually explicit photographs in his sample were taken within the past 10-15 years. The frightening fact is that 15% yielded 300 – 350 children who have been photographed within the last 10-15 years whilst being subjected to serious sexual assaults, then those photographs have been made publicly available: Max Taylor "The Nature and Dimensions of Child Pornography on the Internet" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999) <http://www.stop-childpornog.at/pa_taylor.html> (last accessed 3 May 2001).

[48] See Max Taylor "The Nature and Dimensions of Child Pornography on the Internet" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999) <http://www.stop-childpornog.at/pa_taylor.html> (last accessed 3 May 2001).

[49] Max Taylor "The Nature and Dimensions of Child Pornography on the Internet" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999) <http://www.stop-childpornog.at/pa_taylor.html> (last accessed 3 May 2001).

> experience. It's a natural progression. Like stealing. You start small. Get bored. Go for bigger stuff."

(c) The reproduction of objectionable material without loss of quality and the production of material including morphed images (pseudo children).[50]

The reproduction of material by digital means ensures that duplicated material is as clear as the original. With physical copies of objectionable material, the copies deteriorate.[51] Eventually the copies become so indecipherable that there is no point in attempting to reproduce further copies: eventually there is a limit to the number of users. However, with digital material there are no limitations on the numbers of end users.

Digital production techniques also overcome the pre-existing requirement that new material be physically produced. The potential for the production of new material through morphed children has greatly increased the potential for new images being produced and circulated. That may be seen as a potentially good result: digitally produced child pornography limits the

---

[50] The Head of the Trafficking in Human Beings Branch, Interpol, classified the growth of information technology as making the "production of child pornography into a sophisticated, world-wide 'cottage industry'": Agnès Fournier de Saint Maur "The Sexual Abuse of Children via the Internet: a New Challenge for Interpol" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999) <http://www.stop-childpornog.at/ab_maur.asp> (last accessed 3 May 2001).

[51] Be it books being photocopied or videos being dubbed.

exploitation of real children. The process of habituation, however, belies that apparently advantage and as *News Media* stated, "the minds of some will . . . turn to the real thing".[52]

(d) A level of anonymity through merely being identified by an IP address or by using technology aimed at providing extra anonymity. Simple techniques for avoiding being identified by an IP address include providing false details. It is common for ISPs not to check the validity of the details supplied to it.[53] Specific technological tools include anonymous remailers and on-the-fly or dynamically assigned IP addresses. Of course, venues such as cybercafes also provide a level of anonymity for distribution of material, but understandably, they do not provide the requisite privacy for using the material.

(e) A greater level of control both in the material selected and the medium of storage, in particular the capability to use detection evasion techniques. Detection evasion techniques include simple mechanisms such as password protection, enlarging the computer's cache to enable downloaded material to be retained without saving (which

---

[52] *News Media Ltd v Film and Literature Board of Review* (1997) 4 HRNZ 410, 420.
[53] Edwin C MacGillavry "Internet Service Providers and Criminal Investigation" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October

allows the user to claim no knowledge of the material), and ability to delete data almost instantaneously, although complete wiping of evidence requires a little more knowledge.

(f) The opportunity for greater security through certain protocols. Those protocols include encryption, bot controlled servers to restrict access, "invisible" IRC (Internet relay chat) video conferencing protocols such as CUSeeMe (also known as CU C Me), and direct connections on closed networks to enable file sharing.

(g) A virtual community to reinforce the belief systems and behaviours related to the use of child pornography.

(h) The potential for participation in real-time sexual activity with children. An example of such activity was the technology-facilitated abuse of children by the members of the Orchid Club:[54]

> The Orchid Club was a group of sixteen male child sex abusers coming from several different countries united only by their paedophilia. Each of these men had a video camera attached to their screens which enabled them together to watch a girl of 10

1999) <http://www.stop-childpornog.at/pa_gillavry.html> (last accessed 3 May 2001).

[54] Ron O'Grady "Opening Address" (Child Pornography on the Internet Experts Meeting, Lyon, 28 May 1998) <http://www.ecpat.net/Childporn/Ron's.html> (last accessed 14 May 2001). See also Alexander Wood "National Crime Squad, United Kingdom - Briefing Note" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999) <http://www.stop-childpornog.at/ab_maur.asp> (last accessed 3 May 2001).

> years being sexually abused in real time. They could directly participate in the abuse while it was taking place by offering suggestions and encouragement to the abuser.

C Conclusion

All these features present challenges for policing both in terms of investigating and prosecuting offences under the FVPCA.

V INVESTIGATORY CHALLENGES

A Introduction

The investigatory challenges obviously are greatest where there are "gaps" in investigatory powers. The "gaps" arise from the fact that the FVPCA framework did not foresee the need for more responsive investigatory tools. The provisions enacted were deemed satisfactory to meet "real-world" objectionable material issues.

The features of the Internet that are advantageous to those using and dealing in child pornography were not relevant to child pornography in physical form. While the Act attempted to deal in technologically neutral terms, there were no means to predict the specific advantages that exist by means of the Internet today.

One of the biggest investigatory challenges is having adequate resources to address the special challenges that cyberspace presents. However, this is not the forum for that debate. The following discussion will aim to identify the technical and legal difficulties that the Internet has introduced in respect to enforcing the FVPCA. In all this, it is important to remember that the Act intended to protect children from being exploited sexually by means of the depictions and to prevent paedophiles having a tool at their disposal. Any potential solutions to the various issues need to provide a "balance" to the advantages that the Internet provides for "users" of child pornography if effective policing of that material is to be achieved.

B Jurisdiction

1 Introduction

Obviously, like all aspects of the Internet, jurisdictional issues are to the fore. New Zealand Police have only the power to enforce New Zealand law within New Zealand territory. However, investigating FVPCA offences in cyberspace, at the very least, increases the potential for inquiries to lead overseas.

While Police are not totally devoid of options when investigating trans-boarder offending, the traditional means of receiving evidence from overseas have inherent weaknesses that do

not facilitate effective policing reactions in the age of the instantaneous world wide web.

2 Mutual assistance

The slow, bureaucratic process of the formal international assistance provisions is not available in respect of FVPCA offences. The Mutual Assistance in Criminal Matters Act 1992 requires a penalty of two years' imprisonment under New Zealand law before the benefits of the scheme can be co-opted. The most severe penalty under the FVPCA is one year's imprisonment under section 124 for a person who knowingly undertakes an act that feeds the generation and dissemination process.

3 Interpol

On a more informal basis, Interpol provides a means for requests for inquiries to be conducted in other jurisdictions through Interpol offices around the world. The process to activate offshore inquiries is as follows. New Zealand Police send a request to the Interpol office in Wellington, which, in turn, sends it to relevant extra-jurisdictional Interpol office. That office then forwards the request to the local law enforcement agency for follow up. Any results are returned via the reverse conduits.

The results of such requests are heavily dependent on the local agency's resources and the local laws enabling the inquiries requested

to be made. While not as limited in application as the Mutual Assistance scheme, the process is unpredictable in the sense of what response will be achieved and in what timeframe. Just as importantly, the evidential viability of information collected is dependant on the methodology used by the foreign officers in collecting the information sought and the ability to adduce satisfactory evidence of such investigations at hearing.[55]

4 International co-operation required

At present the absence of international co-operation in respect of child pornography (except on an ad hoc basis, such as Operation Cathedral)[56] inhibits effective investigation of offences. Effective investigations require formal international co-operation measures that are responsive, in terms of speed and effective in collecting the evidence required to obtain a conviction in New Zealand.[57]

---

[55] For example, via video link, or some such method, without prohibitory costs.

[56] Operation Cathedral was a British National Criminal Intelligence Service lead multi-jursidictional co-operative policing operation that broke up an international paedophile ring, the Wonderland Club. It resulted in the imprisonment of seven British men in respect of conspiracy to distribute pornographic images. See "Porn Ring 'was Real Child Abuse'" <http://news.bbc.co.uk/hi/english/uk/newsid_1109000/1109787.stm> (last accessed 3 May 2001) and "Paedophiles Jailed for Porn Ring" <http://news.bbc.co.uk/hi/english/uk/newsid_1168000/1168112.stm> (last accessed 3 May 2001).

[57] In essence there has to be some coincidence of legal frameworks. The European Draft Convention on Cyber-Crime attempts to co-ordinate some standardised provisions which European States can implement: Council of Europe *Draft Convention on Cyber-Crime (Draft 25)* <http://convetnions.coe.int/treaty/EN/projects/cybercrime25.htm> (last accessed 14 May 2001).

C Anonymity

1 Introduction

Anonymity is a perception of the Internet. It does not have to be a fact. Professor Max Taylor put it this way: "[t]he Internet is anonymous only because we allow it to be".[58] Generally, identification information does attach to Internet use. The difficulty is obtaining it and making sure it is accurate.

2 Legislative action required

In the absence of a legal requirement to record accurate client details, for any access to the Internet, those who do not want to be identified will attempt find means of avoiding the connection between themselves and an account number on an ISP. Simple deception measures such as lying, if details are not checked, can defeat accurate identification of IP number holders.

One other method of identification, which, until wireless application technology is functional in a widespread context, will be valuable, is calling line identification. Calling line identification is the information that identifies the telecommunication landline that the computer in question is using to access the Internet. That always has a

---

[58] Max Taylor "The Nature and Dimensions of Child Pornography on the Internet" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999) <http://www.stop-childpornog.at/pa_taylor.html> (last accessed 3 May 2001).

physical point of origin. By nature, it always leads to a specific address.[59]

Identity information, be it names and addresses (which are linked to IP addesses and calling line identification),[60] can be collected from New Zealand based ISPs by means of:

(a) Disclosure made by the ISP under Information Privacy Principle ("IPP") 11(e)(i), section 6 Privacy Act 1993;[61] or

(b) A FVPCA warrant,[62] so long as the identification information sought is *evidence* of an offence, not just information.

However, data of that nature has to be first collected and stored by the ISP. If it is not, or if it is destroyed too quickly, that lead will be lost. It would seem appropriate that some means of preserving such data be developed. Whether it be by legislative imposition or industry agreement, the greater the information resources available to the investigating officers, the greater the likelihood of success. At

---

[59] Edwin C MacGillavry "Internet Service Providers and Criminal Investigation" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999) <http://www.stop-childpornog.at/pa_gillavry.html> (last accessed 3 May 2001).

[60] Edwin C MacGillavry "Internet Service Providers and Criminal Investigation" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999) <http://www.stop-childpornog.at/pa_gillavry.html> (last accessed 3 May 2001). That may change as wireless application technology develops.

[61] That IPP enables disclosure if the organisation has reasonable grounds for believing that disclosure is necessary to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences.

present, there is no statutory requirement or industry agreement that ISPs capture any such data, let alone that the ISP store it to be accessible in the investigation of offences.

3 International co-operation necessary

International ISPs, of course, cause the usual difficulties with lack of jurisdiction.[63] As Operation Cathedral showed, however, even in countries where there lacked means to gain disclosure of accurate IP account holder details, determined and co-operative police work could lead to the identification of the offenders, even those who were very careful not to be identified. The limitation on such an ad hoc approach is that operation was very resource intensive and unlikely to be achievable in respect of single suspects offending against the FVPCA.

D Expanse of the Internet

1 Introduction

Another issue is how to locate objectionable material on the Internet that is not presently being traded or otherwise disseminated so as to be locatable during transmission. "Accidental discovery" under section 108 FVPCA may be satisfactory to locate physical

---

[62] Of course, where the offence being investigated is mere possession, an FVPCA warrant is not available.

[63] However, California permits the execution of search warrants based on overseas search warrants, without relying on the formal Mutual Assistance provisions.

publications but it is not a finely tuned investigation tool in an ever-expanding electronic environment.

New Zealand Parliamentarians have acknowledged that paedophiles use such material to condition their victims. It would be logical to deprive paedophiles of such tools before they can be used. Why leave such material in society so that when it is used, whether to "excite" or "condition",[64] it amounts to a revictimisation of those depicted? Why would one leave the removal of that material to chance when in the Internet setting it could be so readily reproduced and distributed?

2 ISPs and check sum programs

(a) Check sum programs

There is the technology available to have ISPs audit their own servers. The German Federal Criminal Police have had an ISP trial software called PERKEO.[65] The software produces check sums of files classified as definite pornography. In essence, a file can be identified as being identical to a known file by the check sum it produces.[66] While even an alteration as small as changing the size of a picture will produce a different check sum, the automated process is

---

[64] To use Hon Jenny Shipley's words: Hon J Shipley (2 December 1992) 532 NZPD 12760.

[65] Holger Kind "Combating Child Pornography on the Internet by the German Federal Criminal Police Office" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999) <http:// www.stop-childpornog.at/pa_kind.html> (last accessed 3 May 2001).

[66] That is the numerical value based on the number of set bits in the file when the same formula is applied to the file. "Checksum" Webopedia <http://www. webopedia.com/TERM/c/checksum.html> (last accessed 18 June 2001).

far quicker and more accurate in locating files previously identified as pornographic than manual means. According to the German Federal Criminal Police trials, PERKEO is an effective and efficient means of locating child pornography.

(b) Mandatory disclosure of results required

Having ISPs conduct electronic checks of the data they have control of to identify child pornography would appear a logical and effective step to be taken. Whether that is achieved by legislative requirement or self regulation by ISPs, the law enforcement outcomes would be negligible without the ability to have the results of each audit disclosed to enable Police to locate objectionable material and act upon it.

While ISPs can release the material to Police under IPP 11(e)(i), section 6 Privacy Act 1993, such a release is dependant on the individual ISP's perspective of the material and its consideration of whether it should release the information. Attempting to execute section 109 search warrants in respect of every PERKEO-type search would be logistically impossible, given that effective use of PERKEO requires an ongoing process. New warrants would have to be continually sought, as the section 109 warrant only covers evidence presently in existance, not evidence created in the future by the continual re-execution of the check sum program.

Legislative provisions requiring such checks to be conducted and the results to be disclosed to Police appear to be the most effective method of ensuring such information is available for law enforcement purposes.

(c) International co-operation

Obliging New Zealand ISPs to conduct such audits of their servers is one step towards locating objectionable material within New Zealand's jurisdiction. However, New Zealand users can and do use the services of international ISPs. Again, jurisdictional issues arise. Without consistent domestic provisions in the countries where New Zealanders' foreign ISPs are located, the power to locate known pornographic material that may have come into New Zealand would be diluted. While the enactment of such provisions in other jurisdictions is out of the New Zealand Legislature's control, this fact reinforces the realisation that without concerted international co-ordination in respect of the appropriate legislative approach, readily identifiable child pornography will remain in circulation.

3 Hotlines and tiplines

In conjunction with having ISPs complete audits of their servers, "Hotlines" and "tiplines" would appear to be another means of lessening the daunting task of locating objectionable material stored within the confines of the Internet. Just like any other offence, public

reporting provides an effective means of detection.[67] The potential invisibility of objectionable material on the Internet, at least as far as law enforcement agencies are concerned, given its vastness, provides an opportunity for reporting to play a significant role.

E Surmounting Technological Evasion Techniques

1 Technological advantage

Two things, at the very least, must happen if one is serious about minimising the exploitation of children and young persons through pornography: detection and prevention.

To ensure detection is possible, the technological means that permit paedophiles active on the Internet to evade detection must be matched and surpassed by the technological investigation tools at Police disposal. In respect of preventing the further exploitation of children, the closed groups which paedophiles form need to be penetrated and intervention effected by prosecutions based upon evidence gathered. Given that such groups are subject to technological protection both by the communication techniques they use and the technology they use to prevent access by unknown

---

[67] The Department of Internal Affairs has a Tipline email address to which sites containing objectionable material can be reported: censorship@dia.govt.nz: Department of Internal Affairs *Censorship and the Internet* (Wellington, 2001) <http://www.censorship.dia.govt.nz/DIAwebsite.nsf/c7ad5e032528c34c4c2566690076db9b/df667ab0dc96f927cc2568f7007cb1d1!OpenDocument> (last accessed 20 June 2001). Overseas experience, however, suggests that 80% of reports to such facilitates are about non-objectionable content. However, it does provide another tool in the attempt to minimise the exploitation of children and young person.

persons when they are "absent" from their group, technological capability is required to effectively defeat their evasion and security mechanisms.

2 Lawful authority to use

However, there is no point in having the latest technology, if it cannot be used lawfully. The New Zealand Bill of Rights Act 1990 requires that all search and seizures be conducted reasonably: section 21. Caselaw has held that while reasonableness and lawfulness are not synonymous, generally a search will be reasonable if it is lawful.[68] Ensuring the admissibility of any evidence seized through the use of investigative technologies will be dependent on legislation.

Any legislative action needs to acknowledge that there are some technological means of evading detection that cannot presently be circumvented, such as 128-bit encryption. Thus, it is preferable that any provisions enacted should:

(a) Require ISPs to provide encryption keys to unlock protected files.[69] The power to obtain actual encryption keys or other means of "unlocking" security protection protocols, such as passwords, would be a last resort. It

[68] *R v Jefferies* [1994] 1 NZLR 290; (1993) 10 CRNZ 202 (CA) and more recently *R v Grayson and Taylor* [1997] 1 NZLR 399 (CA), also reported as *R v Grayson* (1996) 3 HRNZ 250 (CA) , also reported as *R v Taylor* (1996) 14 CRNZ 426 (CA).

would be preferable to legislate for a range of means to enable enforcement agencies to obtain the information really sought: the contents of protected files.[70]

Any such provision would have to be drafted carefully to ensure that technologically neutral wording was used to prevent the powers becoming obsolete. The key focus of the provision should be obtaining the contents of the file, which Police, but for the presence of the security protocol, would have seized and been able to examine.

(b) Extend interception warrants to cover the computer-based communications of child pornographers.[71]

Police can intercept evidence of criminal activity under Part XIA Crimes Act 1961 and sections 14-29 Misuse of Drugs Amendment Act 1978. However, those provisions are limited to specific offences and, at present,[72] are only applicable to audible communications. Clearly, being able to monitor communications between users of child

---

[69] Part III, Regulation of Investigatory Powers Act 2000 in the United Kingdom requires the disclosure of encryption keys, or at least the unencrypted file.

[70] ISPs that have control of protected files could, for example, simply decrypt or unlock the file and provide that unprotected data directly to the Police.

[71] Presently such an intercept could only be authorised for quasi-FVPCA purposes in respect of the making of a publication where a child was being subjected to sadistic sexual violation. That would be the only means to get the sexual exploitation of a child with the serious violence provisions as defined by section 312A Crimes Act 1961.

[72] The Crimes Amendment Bill (No 6), presently before the Parliament, plans to extend the existing intercept to computer communications.

pornography has advantages from a child protection perspective and in providing the evidence to destroy paedophile networks.

(c) Provide for traffic data warrants. Traffic data warrants are akin to call data warrants.[73] The warrants authorise information pertaining to a target computer's interactions to be gathered as the interactions occur.

In the sense that it allows the undetected instantaneous observation of a computer user's activities, it serves as a means to prevent child pornographers "tipping off" their contacts about Police interest. It allows Police to act in respect to all suspected members of a child pornography ring when terminating an operation, without providing a window of opportunity for other members to destroy evidence.[74]

Each suggested extension of offline search and seizure powers gives rise to concerns as to the abridgement of individual rights.

---

[73] Sections 10A – 10S Telecommunications Act 1987.
[74] As would be the case with search warrants executed on one member alone.

However, as section 5 New Zealand Bill of Rights Act 1990 indicates, there are no absolute rights. If properly enacted, such powers will be lawful and reasonable restrictions on individual freedoms.

The European Community, which maintains strict observance of human rights, is on the verge of concluding a Convention on Cyber-Crime requiring its member States to enact such investigatory powers.[75] In doing so, the European Community has recognised the need for comparable procedural provisions to ensure effective trans-national enforcement of child pornography laws. To effectively contribute to the international community's fight against child pornography, New Zealand must enact comparable provisions.

Incorporating such investigatory powers within the FVPCA both minimises the costs of investigations and lowers the risk that child pornographers would uncover any other means of investigation.[76]

---

[75] The enactment of traffic data and interception provision is demanded by the Draft Convention on Cyber-Crime (Draft 25). Article 20 requires legislative provision to be made for the collection of traffic data; article 21 provides for the interception of contents: Council of Europe *Draft Convention on Cyber-Crime (Draft 25)* <http://convetnions.coe.int/treaty/EN/projects/cybercrime25.htm> (last accessed 14 May 2001).

[76] Specifically, discovering the infiltration of their group by an undercover officer.

VI PROSECUTORIAL CHALLENGES

A Introduction

The issues under this head are less about illustrating weakness in the current legislation and more about establishing the areas of continuity with offline law and how that might shape prosecution of cases relating to cyberspace objectionable material offences.

B Jurisdiction

1 Deemed jurisdiction

Section 7 Crimes Act 1961 provides an exception to the general rule that acts or omission outside New Zealand territory will not be within the jurisdiction of New Zealand Courts.[77] Section 7 amounts to a deeming provision. Provided that:

(a) An act or omission forming part of the actus reus;[78] or

(b) An event necessary for the completion of any (result) offence;

occurs within New Zealand, New Zealand Courts will be deemed to have jurisdiction.

---

[77] Section 6 Crimes Act 1961.

2 Standard of proof required

This raises an interesting preliminary issue. Before a Court can hear a charge, the issue of whether there is jurisdiction has to be determined. As yet, there appears to be no precedent in New Zealand to determine what standard of proof is required to establish jurisdiction. It is a preliminary issue and, generally, preliminary issues are determined on the balance of probabilities. The Australian Courts have taken that approach to the issue.[79] The Canadian Supreme Court has also adopted that standard of proof.[80]

3 What acts will be sufficient to establish deemed jurisdiction?

That preliminary issue aside, *R v Johnston* (1986) 2 CRNZ 289 provides sufficient precedent that the use of delivery services within New Zealand to commit an element of an offence will be sufficient to provide jurisdiction. By analogy, therefore, the use of a New Zealand based ISP to deliver (in terms of the meaning of "distribute" under section 122) objectionable material will give New Zealand Courts jurisdiction over an offence under section 123(1)(b).[81] International

---

[78] *Tipple v Pain* [1983] NZLR 257; *Collector of Customs v Kozanic* (1983) 1 CRNZ 135.

[79] *R v Thompson* (1989) 169 CLR 1, 41 A Crim R 134; *R v Weissensteiner* (1992) 62 A Crim R 96.

[80] *R v Finta* (1994) 112 DLR (4th) 513; 88 CCC (3d) 417 (SCC). However, that case went further to hold that if "jurisdictional facts" went to an element of the offence then they had to be proved beyond reasonable doubt as part of the prosecution case. That may be no more that requiring that, like any information laid in New Zealand, the phrase referring to the offence's location, must be proved as an element of the offence. If jurisdiction has been able to be established, there should be real no difficulties in establishing location facts beyond reasonable doubt.

[81] That is because the very act of electronic forwarding of the publication amounts also to an act of copying.

support is found for that proposition in the cases such as *R v Governor of Brixton Prison ex p Levin* and *R v Winfield and Lipohar*.[82]

4 Establishing physical control

Of course, establishing jurisdiction is meaningless without achieving physical control over the perpetrator of the offence. Extradition is a topic in and of itself, and cannot be fully examination here. With respect to corporate entities, the Court can exercise control if it has a representative within New Zealand.[83]

C Evidence

1 Ensuring authenticity

In any criminal proceedings, the Court must be satisfied as to the integrity of the evidence before a finding of guilt can be made to a standard of beyond reasonable doubt. A break in the chain of evidence can prove fatal to a prosecution. These concerns are heightened by the malleability of electronic data. Expert evidence may be presented to enable the Court to satisfy it that the evidence presented before it has authenticity. The processes used in the investigation, search, seizure, and custody processes will need to be

---

[82] *R v Governor of Brixton Prison ex p Levin* [1997] QB 65: where instructions were sent from a computer in a foreign jurisdiction the receipt of the electronic instructions by a United States computer was held to be an act done in the United States. *R v Winfield and Lipohar* (1998) 70 SASR 300, as affirmed by the High Court of Australia in (1999) 109 A Crim R 207. There the receipt of a fax in an Australian jurisdiction amounted to an act done within that jurisdiction.

[83] Corporations, not being physical entities, must appear in Court by means of a representative: section 2 Summary Proceedings Act 1957.

demonstrated as being technically robust, so that the Court can reach the conclusion that the data has not been compromised in anyway.

2 Ensuring comprehension

Expert evidence is not only needed to establish evidential authenticity. It is also required to enable the Court to comprehend how the offence was committed, where technical aspects may serve to provide a "defence by confusion". Thus, prosecution experts must not only be technically qualified, but also effective communicators.

(a) Cache alterations: an example

One particular example demonstrates the benefits of relying on technical evidence where an offence may not have been obvious to a finder of fact not conversant in technological matters. While possession under section 131 is a strict liability offence, that strict liability relates to awareness of the contents: knowledge or reasonable grounds to believe. The fact of possession still needs to be proved.

In general criminal matters, possession requires both physical control and a mental element. "A person cannot possess something of which he [or she] is unaware".[84] Such logic, thus, requires some indication of a person's awareness that he or she has material under his or her control (independent of his or her awareness of the contents). This point is particularly germane to the operation of the

[84] *Julian v Green* (1989) 5 CRNZ 97, 98.

cache. Generally, control and intention to possess a file accessed through the Internet can be demonstrated because the file is downloaded and saved, a process which demonstrates intention to possess that file.

However, files that appear in the cache are automatically placed there by the computer's own processes, independent of the user's direct control.[85] A person without computer knowledge would not necessarily consider the cache as capable of being used as part of the computer's permanent memory. However, technically competent individuals can expand the cache's storage capacity and use it as part of the permanent harddrive, without leaving telltale "fingerprints" of knowledge and awareness by manually downloading and saving a particular file.

Thus, comprehensible expert evidence provides the Court with the ability to understand that such alterations to the cache provide evidence of intention to retain files automatically loaded into the cache. Such evidence can rebut a defence of absence of intention to possess.

---

[85] Thus, if someone accesses an Internet site and opens a page on that site, the data contained within that page will be stored in the cache to maximise the efficiency of the computer.

V CONCLUSION

The Internet has revolutionised the manner in which child pornography can be produced, obtained, stored, and dealt with. In doing so it has raised some novel issues as to how investigations and prosecutions under the FVPCA can be carried out to achieve the Act's initial goal in respect of section 3(2)(a): a ban on child pornography.

In respect of the investigative issues, conventional policing has few responses to the advantages that the Internet supplies to users of child pornography. While innovative policing options are available,[86] consistency and certainty in both the investigative outcomes and the viability of evidence obtained are not guaranteed without legislative intervention. The prosecutorial issues, however, are more consistent with offline problems. They appear more amenable to conventional resolution through practical means, such as presenting detailed but comprehensible evidence through an appropriately qualified expert.

Of course, the international dimension of the Internet provides the most challenging difficulty. While it is not New Zealand's place to police the whole of the Internet, New Zealand should be active within the international community. Other nations should be

---

[86] Such as providing PERKEO software to ISPs for monitoring of content.

encouraged to enact consistent investigatory powers and international co-ordination in response to child pornography should be championed.

While legislative action is a necessary step in achieving the objective of banishing child pornography from New Zealand, it is hopefully clear that child pornography on the Internet, as it impacts in New Zealand, is not just an enforcement agency responsibility. New Zealand Police work under a Strategic Plan, which has as its central philosophy "Safer Communities Together". While it has not been the purpose of this paper to examine issues of self-regulation, just like real-world communities, those who choose to participate in the online world, including all the stakeholders,[87] need to collaborate in making it a "safer community". That concept is highly relevant to the online community in which offending can be potentially invisible to law enforcement authorities:[88]

> The fight against this abuse [child pornography] cannot be done alone but only through strong international cooperation, among governments, particularly law enforcement agencies, but equally important between States and the Internet industry, hotlines and non-governmental organisation.

---

[87] Internet users, ISPs, Parliament, enforcement agencies, both nationally and internationally, and voluntary watchdog organisations.

[88] "Conclusions and Recommendations of the International Conference 'Combating Child Pornography on the Internet'" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999) <http://www.stop-childpornog.at/pa_kind.html> (last accessed 3 May 2001).

APPENDIX – LEGISLATIVE PROVISIONS

I FILMS, VIDEOS, AND PUBLICATIONS CLASSIFICATION ACT 1993

Section 2 Interpretation

"Publication" means—

(a) Any film, book, sound recording, picture, newspaper, photograph, photographic negative, photographic plate, or photographic slide:

(b) Any print or writing:

(c) Any paper or other thing—

(i) That has printed or impressed upon it, or otherwise shown upon it, any word, statement, sign, or representation; or

(ii) On which is recorded or stored any information that, by the use of any computer or other electronic device, is capable of being reproduced or shown as any word, statement, sign, or representation.

"**Supply**" means to sell, or deliver by way of hire, or offer for sale or hire.

Section 3 Meaning of "objectionable"

(1) For the purposes of this Act, a publication is objectionable if it describes, depicts, expresses, or otherwise deals with matters such as sex, horror, crime, cruelty, or violence in such a manner that the availability of the publication is likely to be injurious to the public good.

(2) A publication shall be deemed to be objectionable for the purposes of this Act if the publication promotes or supports, or tends to promote or support,—

(a) The exploitation of children, or young persons, or both, for sexual purposes; or

(b) The use of violence or coercion to compel any person to participate in, or submit to, sexual conduct; or

(c) Sexual conduct with or upon the body of a dead person; or

(d) The use of urine or excrement in association with degrading or dehumanising conduct or sexual conduct; or

(e) Bestiality; or

(f) Acts of torture or the infliction of extreme violence or extreme cruelty.

(3) In determining, for the purposes of this Act, whether or not any publication (other than a publication to which subsection (2) of this section applies) is objectionable or should be given a classification other than objectionable, particular weight shall be given to the extent and degree to which, and the manner in which, the publication—

(a) Describes, depicts, or otherwise deals with—

(i) Acts of torture, the infliction of serious physical harm, or acts of significant cruelty:

(ii) Sexual violence or sexual coercion, or violence or coercion in association with sexual conduct:

(iii) Other sexual or physical conduct of a degrading or dehumanising or demeaning nature:

(iv) Sexual conduct with or by children, or young persons, or both:

(v) Physical conduct in which sexual satisfaction is derived from inflicting or suffering cruelty or pain:

(b) Exploits the nudity of children, or young persons, or both:

(c) Degrades or dehumanises or demeans any person:

(d) Promotes or encourages criminal acts or acts of terrorism:

(e) Represents (whether directly or by implication) that members of any particular class of the public are inherently inferior to other members of the public by reason of any characteristic of members of that class, being a characteristic that is a prohibited ground of discrimination specified in section 21(1) of the Human Rights Act 1993.

(4) In determining, for the purposes of this Act, whether or not any publication (other than a publication to which subsection (2) of this section applies) is objectionable or should be given a classification other than objectionable, the following matters shall also be considered:

(a) The dominant effect of the publication as a whole:

(b) The impact of the medium in which the publication is presented:

(c) The character of the publication, including any merit, value, or importance that the publication has in relation to literary, artistic, social, cultural, educational, scientific, or other matters:

(d) The persons, classes of persons, or age groups of the persons to whom the publication is intended or is likely to be made available:

(e) The purpose for which the publication is intended to be used:

(f) Any other relevant circumstances relating to the intended or likely use of the publication.

Section 108 Seizure of objectionable publications

(1) Subject to subsection (2) of this section, where an Inspector or a member of the Police, in the course of carrying out his or her lawful duties, discovers any publication that he or she believes, on reasonable grounds, to be objectionable, that person may, without further authority than this section, seize that publication.

(2) Nothing in subsection (1) of this section applies to any publication that is in the possession of any person in circumstances in which, by virtue of subsection (4) or subsection (5) of section 131 of this Act, the possession of that publication by that person is not an offence against subsection (1) of that section.

Section 109 Search warrants

(1) Any District Court Judge[, Justice, or Community Magistrate], or any Registrar (not being a member of the Police), who, on an application in writing made on oath, is satisfied that there are reasonable grounds for believing that there is in or on any place or thing—

(a) Any objectionable publication that there are reasonable grounds to believe is being kept for the purpose of being so dealt with as to constitute an offence against section 123 or section 124 or section 127 or section 129 of this Act; or

(b) Any thing that there are reasonable grounds to believe will be evidence of the commission of such an offence; or

(c) Any thing that there are reasonable grounds to believe is intended to be used for the purpose of committing such an offence—

may issue a search warrant.

(2) An application under subsection (1) of this section may be made by any Inspector or any member of the Police.

Section 122 Interpretation

In sections 123 to 132 of this Act, unless the context otherwise requires, the term "distribute" means to deliver, to give, or to offer.

Section 123 Offences of strict liability relating to objectionable publications

(1) Every person commits an offence against this Act who—

(a) Makes an objectionable publication; or

(b) Makes a copy of an objectionable publication for the purposes of supply, distribution, display, or exhibition to any other person; or

(c) Supplies, or has in that person's possession for the purposes of supply, an objectionable publication; or

(d) For the purposes of supply to any other person, distributes, displays, advertises, or exhibits an objectionable publication; or

(e) In expectation of payment, or otherwise for gain, or by way of advertisement, distributes, displays, exhibits, or otherwise makes available an objectionable publication to any other person; or

(f) Delivers to any person an objectionable publication with intent that it should be dealt with by that person or any other person in such manner as to constitute an offence against this section or section 124 or section 127 or section 129 of this Act.

(2) Every person who commits an offence against subsection (1) of this section is liable to a fine not exceeding,—

(a) In the case of an individual, $5,000:

(b) In the case of a body corporate, $15,000.

(3) It shall be no defence to a charge under subsection (1) of this section that the defendant had no knowledge or no reasonable cause to believe that the publication to which the charge relates was objectionable.

(4) Without limiting the generality of this section, a publication may be—

(a) Supplied (within the meaning of that term in section 2 of this Act) for the purposes of paragraphs (b), (c), and (d) of subsection (1) of this section; or

(b) Made available for the purposes of paragraph (e) of that subsection—

not only in a physical form but also by means of the electronic transmission (whether by way of facsimile transmission, electronic mail, or other similar means of communication, other than by broadcasting) of the contents of the publication.

Section 124 Offences involving knowledge in relation to objectionable publications

(1) Every person commits an offence against this Act who does any act mentioned in section 123(1) of this Act, knowing or having reasonable cause to believe that the publication is objectionable.

(2) Every person who commits an offence against subsection (1) of this section is liable,—

(a) In the case of an individual, to imprisonment for a term not exceeding 1 year or to a fine not exceeding $20,000:

(b) In the case of a body corporate, to a fine not exceeding $50,000.

Section 131 Offence to possess objectionable publication

(1) Subject to subsections (4) and (5) of this section, every person commits an offence against this Act who, without lawful authority or excuse, has in that person's possession an objectionable publication.

(2) Every person who commits an offence against subsection (1) of this section is liable to a fine not exceeding,—

(a) In the case of an individual, $2,000:

(b) In the case of a body corporate, $5,000.

(3) It shall be no defence to a charge under subsection (1) of this section that the defendant had no knowledge or no reasonable cause to believe that the publication to which the charge relates was objectionable.

(4) Nothing in subsection (1) of this section makes it an offence for any of the following persons to be in possession of an objectionable publication, where such possession is for the purpose of and in connection with the person's official duties:

(a) The Chief Censor:

(b) The Deputy Chief Censor:

(c) Any classification officer:

(d) Any person holding office pursuant to clause 2 of the First Schedule to this Act:

(e) Any member of the Board:

(f) The labelling body or any person who is carrying out the functions of the labelling body:

(g) Any Inspector:

(h) Any member of the Police:

(i) Any officer of the Customs:

(j) Any Judge of the High Court, or District Court Judge, Coroner[, Justice, or Community Magistrate]:

(k) In relation to any publication delivered to the National Librarian pursuant to [section 30A of the National Library Act 1965],

the National Librarian, any other employee of the National Library Department, or any person employed in the Parliamentary Library:

(l) Any other person in the service of the Crown.

(5) It is a defence to a charge under subsection (1) of this section if the defendant proves that the defendant had possession of the publication to which the charge relates, in good faith,—

(a) For the purpose or with the intention of delivering it into the possession of a person lawfully entitled to have possession of it; or

(b) For the purposes of any proceedings under this Act or any other enactment in relation to the publication; or

(c) For the purpose of giving legal advice in relation to the publication; or

(d) For the purposes of giving legal advice, or making representations, in relation to any proceedings; or

(e) In accordance with, or for the purpose of, complying with any decision or order made in relation to the publication by the Chief Censor, the Classification Office, the Board, or any court, Judge[, Justice, or Community Magistrate]; or

(f) In connection with the delivery of the publication to the National Librarian in accordance with [section 30A of the National Library Act 1965].

(6) Nothing in subsection (5) of this section shall prejudice any defence that it is open to a person charged with an offence against this section to raise apart from that subsection.

(7) For the avoidance of doubt, in this section the term ``proceedings'' includes proceedings before the Classification Office.

Section 142 Offences punishable on summary conviction

Every offence against this Act or any regulations made under this Act shall be punishable on summary conviction.

Section 143 Extending time for taking prosecutions

Notwithstanding anything in section 14 of the Summary Proceedings Act 1957, any information in respect of any offence against this Act may be laid at any time within 2 years after the time when the matter of the information arose.

Section 144 Leave of Attorney-General to prosecute

(1) No prosecution for an offence against any of sections 123 to 129 of this Act or against section 131 or section 133 of this Act shall be commenced except with the leave of the Attorney-General.

(2) The Attorney-General may delegate the powers of the Attorney-General under subsection (1) of this section to the Commissioner of Police in respect of offences concerning any particular class of publications.

(3) The Commissioner of Police, in purporting to act under any delegation under subsection (2) of this section, shall, in the absence of proof to the contrary, be presumed to be acting within the terms of the delegation.

(4) Any such delegation may be at any time revoked by the Attorney-General, in whole or in part, but that revocation shall not affect in any way anything done under the delegated authority.

(5) No such delegation shall prevent the exercise by the Attorney-General of any power under subsection (1) of this section.

Section 145 Delegation of powers by Commissioner of Police

(1) The Commissioner of Police may from time to time, by writing under the Commissioner's hand, either generally or particularly, delegate to such member or members of the Police, of a rank not less than Inspector, as the Commissioner thinks fit, all or any of the powers delegated to the Commissioner under section 144 of this Act.

(2) Every person purporting to act pursuant to any delegation under this section shall be presumed to be acting in accordance with the terms of the delegation in the absence of proof to the contrary.

(3) Subject to subsection (1) of this section, any delegation under this section may be made to a specified member of the Police or to members of the Police of a specified rank or class, or may be made to the holder or holders for the time being of a specified office or class of offices.

(4) Every delegation under this section shall be revocable at will, and no such delegation shall prevent the exercise of any power by the Commissioner of Police.

(5) Any such delegation shall, until revoked, continue in force according to its tenor, notwithstanding the fact that the Commissioner of Police by whom it was made may have ceased to hold office, and

shall continue to have effect as if made by the successor in office of that Commissioner.

(6) The revocation of any such delegation shall not affect in any way anything done under the delegated authority.

II CRIMES ACT 1961

Section 6 Persons not to be tried in respect of things done outside New Zealand

Subject to the provisions of section 7 of this Act, no act done or omitted outside New Zealand is an offence, unless it is an offence by virtue of any provision of this Act or of any other enactment.

Section 7 Place of Commission of Offence

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

Section 312A Interpretation—

"Serious violent offence" means any offence—

(a) That is punishable by a period of imprisonment for a term of 7 years or more; and

(b) Where the conduct constituting the offence involves—

(i) Loss of a person's life or serious risk of loss of a person's life; or

(ii) Serious injury to a person or serious risk of serious injury to a person; or

(iii) Serious damage to property in circumstances endangering the physical safety of any person; or

(iv) Perverting the course of justice, where the purpose of the conduct is to prevent, seriously hinder, or seriously obstruct the detection, investigation, or prosecution of any offence—

(A) That is punishable by a period of imprisonment for a term of 7 years or more; and

(B) That involved, involves, or would involve conduct of the kind referred to in any of subparagraphs (i) to (iii).

Section 312B Application by Police for warrant to intercept private communications—

(1) An application may be made in accordance with this section to a Judge of the High Court for a warrant for any member of the Police to intercept a private communication by means of a listening device in any case where there are reasonable grounds for believing that—

[[(a) Any member of an organised criminal enterprise is planning, participating in, or committing, or has planned, participated in, or committed, criminal offences of which at least one is a specified offence, as part of a continuing course of criminal conduct planned, organised, or undertaken by members of that enterprise; and]]

(b) It is unlikely that the Police investigation of the case could be brought to a successful conclusion without the grant of such a warrant.

(2) Every application under subsection (1) of this section shall be made by a commissioned officer of Police, in writing, and on oath, and shall set out the following particulars:

(a) The facts relied upon to show that there are reasonable grounds for believing that—

(i) There is an organised criminal enterprise; and

(ii) Any member of that enterprise is planning, participating in, or committing, or has planned, participated in, or committed, criminal offences of which at least one is [[a specified offence]] as part of a continuing course of criminal conduct planned, organised, or undertaken by members of that enterprise; and

(b) A description of the manner in which it is proposed to intercept private communications; and

(c) The name and address, if known, of the suspect whose private communications there are reasonable grounds for believing will assist the Police investigation of the case, or, if the name and address of the suspect are not known, a general description of the premises or place in respect of which it is proposed to intercept private communications, being premises or a place believed to be used for any purpose by any member of the organised criminal enterprise; and

(d) The period for which a warrant is requested; and

(e) Whichever of the following is applicable:

(i) The other investigative procedures and techniques that have been tried but have failed to facilitate the successful conclusion of the Police investigation of the case, and the reasons why they have failed in that respect; or

(ii) The reasons why it appears that other investigative procedures and techniques are unlikely to facilitate the successful conclusion of the Police

investigation of the case, or are likely to be too dangerous to adopt in the particular case; or

(iii) The reasons why it is considered that the case is so urgent that it would be impractical to carry out the Police investigation using only investigative procedures and techniques other than the interception of private communications.

Section 312C Matters on which Judge must be satisfied in respect of applications—

(1) On an application made in accordance with section 312B of this Act, the Judge may grant an interception warrant if the Judge is satisfied that it would be in the best interests of the administration of justice to do so, and that—

(a) There are reasonable grounds for believing that—

(i) There is an organised criminal enterprise; and

(ii) Any member of that organised criminal enterprise is planning, participating in, or committing, or has planned, participated in, or committed, criminal offences of which at least one is [[a specified offence]], as part of the continuing course of criminal conduct planned, organised, or undertaken by members of that enterprise; and

(b) There are reasonable grounds for believing that evidence relevant to the investigation of the case will be obtained through the use of a listening device to intercept private communications; and

(c) Whichever of the following is applicable:

(i) Other investigative procedures and techniques have been tried but have failed to facilitate the successful conclusion of the Police investigation of the case; or

(ii) Other investigative procedures and techniques are unlikely to facilitate the successful conclusion of the Police investigation of the case, or are likely to be too dangerous to adopt in the particular case; or

(iii) The case is so urgent that it would be impractical to carry out the Police investigation using only investigative procedures and techniques other than the interception of private communications; and

(d) The private communications to be intercepted are not likely to be privileged in proceedings in a Court of law by virtue of any of the provisions of Part III of the Evidence Amendment Act (No 2) 1980 or of any rule of law that confers privilege on communications of a professional character between a barrister or solicitor and a client.

[(2) Without limiting subsection (1), in determining whether or not to issue an interception warrant under this section, the Judge must

consider the extent to which the privacy of any person or persons would be likely to be interfered with by the interception, under the warrant, of private communications.]

Section 312CA Application by Police for warrant to intercept private communications in relation to serious violent offences—

(1) An application may be made in accordance with this section to a Judge of the High Court for a warrant for any member of the Police to intercept a private communication by means of a listening device in any case where there are reasonable grounds for believing that,—

(a) A serious violent offence has been committed, or is being committed, or is about to be committed; and

(b) Where that serious violent offence has yet to be committed, the use of a listening device to intercept private communications is likely to prevent the commission of the offence; and

(c) It is unlikely that the Police investigation of the case could be brought to a successful conclusion or, as the case may be, the commission of the serious violent offence prevented, without the granting of such a warrant.

(2) Every application under subsection (1) must be made by a commissioned officer of Police, in writing, and on oath, and must set out the following particulars:

(a) The facts relied on to show that there are reasonable grounds for believing that,—

(i) A serious violent offence has been committed, or is being committed, or is about to be committed; and

(ii) Where that serious violent offence has yet to be committed, the use of a listening device to intercept private communications is likely to prevent the commission of the offence; and

(b) A description of the manner in which it is proposed to intercept private communications; and

(c) Either,—

(i) The name and address, if known, of the suspect the interception of whose private communications there are reasonable grounds for believing will assist the Police investigation of the case or, as the case may be, prevent the commission of a serious violent offence; or

(ii) If the name and address of the suspect are not known, a general description of the premises or place in respect of which it is proposed to intercept private communications, being premises or a place believed to be used for any purpose by any person—

(A) Whom it is believed has committed, or is committing, or is about to commit, a serious violent offence; or

(B) Whom it is believed was involved, or is involved, or will be involved, in the commission of a serious violent offence; and

(d) The period for which a warrant is requested; and

(e) Whichever of the following is applicable:

(i) The other investigative procedures and techniques that have been tried but have failed to facilitate the successful conclusion of the Police investigation of the case or, as the case may be, to provide assistance in preventing the commission of a serious violent offence, and the reasons why they have failed in that respect; or

(ii) The reasons why it appears that other investigative procedures and techniques are unlikely to facilitate the successful conclusion of the Police investigation of the case or, as the case may be, prevent the commission of a serious violent offence, or are likely to be too dangerous to adopt in the particular case; or

(iii) The reasons why it is considered that the case is so urgent that it would be impractical to carry out the Police investigation using only investigative procedures and techniques other than the interception of private communications.

Section 312CB Matters on which Judge must be satisfied in respect of applications relating to serious violent offences—

(1) On an application made in accordance with section 312CA, the Judge may grant an interception warrant if the Judge is satisfied that it would be in the best interests of the administration of justice to do so, and that—

(a) There are reasonable grounds for believing that,—

(i) A serious violent offence has been committed, or is being committed, or is about to be committed; and

(ii) Where that serious violent offence has yet to be committed, the use of a listening device to intercept private communications is likely to prevent the commission of the offence; and

(b) There are reasonable grounds for believing that,—

(i) Evidence relevant to the investigation of the case will be obtained through the use of a listening device to intercept private communications; or

(ii) Where the serious violent offence has yet to be committed, evidence relevant to the prevention of that offence will be obtained through the use of a listening device to intercept private communications; and

(c) Whichever of the following is applicable:

(i) Other investigative procedures and techniques have been tried but have failed to facilitate the successful conclusion of the Police investigation of the case or, as the

case may be, to provide assistance in preventing the commission of a serious violent offence; or

(ii) Other investigative procedures and techniques are unlikely to facilitate the successful conclusion of the Police investigation of the case or, as the case may be, prevent the commission of a serious violent offence, or are likely to be too dangerous to adopt in the particular case; or

(iii) The case is so urgent that it would be impractical to carry out the Police investigation using only investigative procedures and techniques other than the interception of private communications; and

(d) The private communications to be intercepted are not likely to be privileged in proceedings in a court of law by virtue of any of the provisions of Part III of the Evidence Amendment Act (No 2) 1980 or of any rule of law that confers privilege on communications of a professional character between a barrister or solicitor and a client.

(2) Without limiting subsection (1), in determining whether or not to issue an interception warrant under this section, the Judge must consider the extent to which the privacy of any person or persons would be likely to be interfered with by the interception, under the warrant, of private communications.

Section 312D Contents and term of warrant—

(1) Every interception warrant shall be issued in the [[prescribed form]], and shall—

(a) State the offence or offences in respect of which the warrant is granted; and

[[(b) State,—

(i) In the case of a warrant granted pursuant to section 312C, the name and address of the suspect, if known, whose private communications may be intercepted, or, where the suspect's name and address are not known, the premises or place in respect of which private communications may be intercepted, being premises or a place believed to be used for any purpose by any member of the organised criminal enterprise; or

(ii) In the case of a warrant granted pursuant to section 312CB, the name and address of the suspect, if known, whose private communications may be intercepted, or, where the suspect's name and address are not known, the premises or place in respect of which private communications may be intercepted, being premises or a place believed to be used for any purpose by any person—

(A) Whom it is believed has committed, or is committing, or is about to commit, a serious violent offence; or

(B) Whom it is believed was involved, or is involved, or will be involved, in the commission of a serious violent offence; and]]

(c) Specify the commissioned officer of Police who (with any other member of the Police for the time being assisting the commissioned officer) may intercept the private communications; and

(d) Where the Judge considers it necessary, contain express authority to enter (with force, where necessary) any aircraft, ship, hovercraft, carriage, vehicle, or premises for the purpose of placing, servicing, or retrieving a listening device; and

(e) Contain such additional terms and conditions as the Judge considers advisable in the public interest.

(2) Without limiting subsection (1) of this section, where it is proposed to place a listening device in the residential or business premises of a person who is a barrister or solicitor, or a clergyman, or a registered medical practitioner, the Judge shall prescribe such conditions (if any) as the Judge considers desirable to avoid so far as practicable the interception of communications of a professional character to which the barrister or solicitor or clergyman or registered medical practitioner is a party.

(3) Every interception warrant shall be valid for such period, not exceeding 30 days, as the Judge shall specify in the warrant.

Section 312E Effect of warrant—

Every interception warrant shall have effect, according to its terms, to authorise the interception of private communications by means of a listening device.

Section 312F Renewal of warrants—

(1) Any Judge of the High Court may from time to time grant a renewal of an interception warrant upon application made at any time before the warrant (or any current renewal of the warrant) has expired.

(2) Every application for the renewal of an interception warrant shall be made in the manner provided by section 312B [[or, as the case requires, section 312CA]] of this Act, and shall give—

(a) The reason and period for which the renewal is required; and

(b) Full particulars, together with times and dates, of any interceptions made or attempted under the warrant, and an indication of the nature of the information that has been obtained by every such interception.

(3) Every such application shall be supported by such other information as the Judge may require.

(4) A renewal of an interception warrant may be granted under this section if the Judge is satisfied that the circumstances described in section 312C [[or, as the case requires, section 312CB]] of this Act still obtain.

(5) Every renewal of an interception warrant shall be valid for such period, not exceeding 30 days, as the Judge shall specify in the renewal.

(6) A renewal of an interception warrant may be granted upon an application made within the time prescribed by subsection (1) of this section notwithstanding that the warrant (or any renewal of the warrant) has expired before the application is determined.

(7) Nothing in this section shall prevent a Judge from granting a second or subsequent renewal of an interception warrant upon an application duly made.

Section 312G Emergency permits—

(1) In any case where a Judge is satisfied that circumstances exist that would justify the grant of an interception warrant under section 312C [[or, as the case requires, section 312CB]] of this Act, but the urgency of the situation requires that the interception should begin before a warrant could with all practicable diligence be obtained, the Judge may, orally or in writing, grant an emergency permit for the interception of private communications in respect of particular premises or a particular place and in a particular manner.

(2) Repealed

(3) Any application for an emergency permit may be made orally, but otherwise every such application shall comply with the requirements of section 312B [[or, as the case requires, section 312CA]] of this Act.

(4) Where the Judge grants the application for an emergency permit, the Judge shall forthwith make a note in writing of the particulars of the application. The note shall be filed in the High Court Registry nearest to where the application is made, and shall, for the purposes of section 312H(1) of this Act, be deemed to be a document relating to the application for the permit. The Judge shall also make a note of the terms of the permit.

(5) The provisions of section 312D of this Act, so far as they are applicable and with the necessary modifications, shall apply to emergency permits in the same manner as they apply to interception warrants.

(6) Every emergency permit shall remain valid for 48 hours from the time when it is given, and shall then expire.

(7) On filing the report required by section 312P of this Act, the member of the Police who applied for the emergency permit (or, if that member is not the member filing the report, then the member who is filing the report) may apply to the Judge who granted the permit (or, if that Judge is not the Judge receiving the report, then the Judge who is receiving the report) for a certificate confirming the permit pursuant to subsection (9) of this section.

(8) Where the Police, within the period of 48 hours during which the emergency permit is valid, apply for an interception warrant in place of the permit, the member of the Police applying for the warrant may also apply for a certificate confirming the permit pursuant to subsection (9) of this section.

(9) The Judge to whom an application is made pursuant to subsection (7) or subsection (8) of this section shall issue a certificate confirming the permit if the Judge is satisfied, having regard to the requirements of section 312C [[or, as the case requires, section 312CB]] of this Act, that if the original application for the emergency permit had been an application for an interception warrant, the Judge would have granted a warrant.

(10) For the purposes of section 312M of this Act, an interception of a private communication pursuant to an emergency permit shall be deemed to have been made unlawfully unless the Judge to whom an application is made in accordance with subsection (7) or subsection (8) of this section issues a certificate confirming the permit pursuant to subsection (9) of this section.

Section 312H Security of applications—

(1) As soon as an application for an interception warrant or for a renewal of an interception warrant or for an emergency permit or for a certificate confirming an emergency permit has been determined by the Judge, the Registrar shall place all documents relating to the application (except the warrant or renewal or permit or certificate itself) in a packet, seal the packet, and thereafter keep it in safe custody, subject to the succeeding provisions of this section.

(2) Notwithstanding any enactment or rule of law or rules of Court entitling any party to any proceedings to demand the production of any documents, no such party shall be entitled to demand the production of any documents held in safe custody pursuant to subsection (1) of this section, except in accordance with the succeeding provisions of this section.

(3) Every such party who requires the production of any document held in safe custody pursuant to subsection (1) of this section shall, except in a case to which subsection (9) or subsection (10) of this section applies, apply in writing to the Registrar, who shall forthwith notify the senior Police officer in the district.

(4) If, within 3 days after notice is given to the senior Police officer in the district under subsection (3) of this section, that officer gives written notice to the Registrar that that officer intends to oppose the production of the documents, the Registrar shall refer the matter to a Judge.

(5) Where the senior Police officer in the district does not give such written notice to the Registrar, the Registrar shall produce the documents to the party applying for production.

(6) Where a matter is referred to a Judge pursuant to subsection (4) of this section, both the person requesting production of the documents and the member of the Police opposing production shall be given an opportunity to be heard.

(7) If the Judge is satisfied that information in any document the production of which is in dispute identifies or is likely to lead to the identification of a person who gave information to the Police, or of any member of the Police whose identity was concealed for the purpose of any relevant investigation and has not been subsequently revealed, the Judge may, if the Judge believes it in the public interest to do so, order that the whole or any specified part of the document be not produced.

(8) Subject to the provisions of subsection (7) of this section, the Judge shall order the production of the documents to the party requesting it.

(9) Where a request for the production of any document kept in safe custody pursuant to subsection (1) of this section is made in the course of any proceedings presided over by a Judge and the request is opposed, the Judge shall adjudicate upon the matter as if it had been referred to the Judge pursuant to subsection (4) of this section.

(10) Where such a request is made in the course of any other proceedings, the presiding judicial officer shall forthwith refer the matter to a Judge for adjudication.

(11) Notwithstanding anything in this section, every Judge who is presiding over any proceedings in which the issue of an interception warrant or emergency permit is in issue shall be entitled to inspect any relevant document held under subsection (1) of this section.

312I Destruction of irrelevant records made by use of listening device—

[[(1) Every person who intercepts a private communication in pursuance of an interception warrant or any emergency permit must, as soon as practicable after it has been made, destroy any record, whether written or otherwise, of the information obtained by that interception if none of the information directly or indirectly relates to—

(a) The commission of a specified offence or a conspiracy to commit such an offence; or

(b) The commission of a serious violent offence or a conspiracy to commit such an offence; or

(c) A drug dealing offence or a prescribed cannabis offence (as those terms are defined in section 10 of the Misuse of Drugs Amendment Act 1978).]]

(2) Every person who fails to comply with subsection (1) of this section commits an offence and is liable on summary conviction to a fine not exceeding $500.

Section 312J Destruction of relevant records made by use of listening device—

[[(1) The Commissioner of Police must ensure that every record, whether written or otherwise, of the information obtained by the Police from the interception of a private communication in pursuance of an interception warrant or an emergency permit, being information that relates wholly or partly and directly or indirectly to—

(a) The commission of a specified offence or a conspiracy to commit such an offence; or

(b) The commission of a serious violent offence or a conspiracy to commit such an offence; or

(c) A drug dealing offence or a prescribed cannabis offence (as those terms are defined in section 10 of the Misuse of Drugs Amendment Act 1978),—

is destroyed as soon as it appears that no proceedings, or no further proceedings, will be taken in which the information would be likely to be required to be produced in evidence.]]

(2) Nothing in subsection (1) of this section shall apply to—

(a) Any record of any information adduced in proceedings in any Court, or (in any case where the defendant pleads guilty) of any record of any information that, in the opinion of the Judge to whom the report referred to in subsection (3) of this section is made, would have been adduced had the matter come to trial:

(b) Any record of any information contained in any transcript or written statement given to any person in accordance with section 312L(a) of this Act.

(3) Every report made to a Judge in accordance with section 312P of this Act shall state whether or not subsection (1) of this section has yet been complied with, and, if it has not, the Judge shall give such directions relating to the eventual destruction of the record as the Judge thinks necessary to ensure compliance with that subsection, including a requirement that the Judge be advised when the record has been destroyed.

Section 312K Prohibition on disclosure of private communications lawfully intercepted—

(1) No person who—

(a) Intercepts or assists in the interception of a private communication in pursuance of an interception warrant or emergency permit; or

(b) Acquires knowledge of a private communication as a direct or indirect result of that interception—

shall knowingly disclose the substance, meaning, or purport of that communication, or any part of that communication, otherwise than in the performance of that person's duty.

(2) Every person who acts in contravention of subsection (1) of this section commits an offence and is liable on summary conviction to a fine not exceeding $500.

Section 312L Notice to be given of intention to produce evidence of private communication—

Particulars of a private communication intercepted pursuant to an interception warrant or an emergency permit shall not be received in evidence by any Court against any person unless the party intending to adduce it has given to that person reasonable notice of that person's intention to do so, together with—

(a) A transcript of the private communication where that person intends to adduce it in the form of a recording, or a written statement setting forth the full particulars of the private communication where that person intends to adduce oral evidence of it; and

(b) A statement of the time, place, and date of the private communication, and of the names and addresses of the parties to the communication, if they are known.

Section 312M Inadmissibility of evidence of private communications unlawfully intercepted—

(1) Subject to subsections (2) to (4) of this section, where a private communication intercepted by means of a listening device otherwise than in pursuance of an interception warrant or emergency permit issued under this Part of this Act or of any authority conferred by or

under any other enactment has come to the knowledge of a person as a direct or indirect result of that interception or its disclosure, no evidence so acquired of that communication, or of its substance, meaning, or purport, and no other evidence obtained as a direct or indirect result of the interception or disclosure of that communication, shall be given against any person, except in proceedings relating to the unlawful interception of a private communication by means of a listening device or the unlawful disclosure of a private communication unlawfully intercepted in that manner.

[[(2) Even though certain evidence is inadmissible in criminal proceedings by virtue of subsection (1), a Court may admit that evidence if the following conditions are satisfied:

(a) The proceedings are for—

(i) A specified offence, or a conspiracy to commit a specified offence; or

(ii) A serious violent offence, or a conspiracy to commit such an offence; and

(b) The evidence is relevant; and

(c) The evidence is inadmissible by virtue of subsection (1) merely because of a defect in form, or an irregularity in procedure, in—

(i) The application for or the granting of the interception warrant or emergency permit; or

(ii) The manner in which the evidence was obtained; and

(d) The defect in form or irregularity in procedure—

(i) Was not substantive; and

(ii) Was not the result of bad faith.]]

(3) Subsection (1) of this section shall not render inadmissible against any party to a private communication evidence of that communication that has, in the manner referred to in that subsection, come to the knowledge of the person called to give evidence, if all the parties to the communication consent to that person giving the evidence.

(4) Subsection (1) of this section shall not render inadmissible evidence of a private communication by any person who intercepted that communication by means of a listening device with the prior consent of any party to the communication.

Section 312N Inadmissibility of evidence of private communications lawfully intercepted—

[[(1) Subject to subsection (2), where a private communication intercepted in pursuance of an interception warrant or an emergency permit discloses evidence relating to any offence other than—

(a) A specified offence, or a conspiracy to commit such an offence; or

(b) A serious violent offence, or a conspiracy to commit such an offence,—

no evidence of that communication, or of its substance, meaning, or purport, may be given in any Court.]]

(2) If, in any proceedings for a drug dealing offence [[or a prescribed cannabis offence (as those terms are defined in section 10 of the Misuse of Drugs Amendment Act 1978)]],—

(a) Evidence is sought to be adduced of a private communication intercepted in pursuance of an interception warrant or an emergency permit issued under this Part of this Act; and

(b) The Judge is satisfied, on the evidence then before the Judge,—

(i) That a warrant or permit could have been issued under Part II of the Misuse of Drugs Amendment Act 1978; and

(ii) That the evidence sought to be adduced would have been admissible if the warrant or permit had been issued under that Part of that Act,—

the evidence may be admitted notwithstanding subsection (1) of this section.

[[(3) Subsection (4) applies where,—

(a) In any proceedings for a prescribed cannabis offence (as so defined), a Judge has to decide whether or not evidence relating to the offence can be admitted under subsection (2); and

(b) In order to make that decision, the Judge has to decide the issue of whether or not a warrant or permit could have been issued under Part II of the Misuse of Drugs Amendment Act 1978 in respect of the prescribed cannabis offence.

[[(4) Where this subsection applies, the Judge must decide the issue referred to in subsection (3)(b) as if a warrant or permit could be issued under section 15B or section 19 of the Misuse of Drugs Amendment Act 1978 in respect of a prescribed cannabis offence regardless of whether or not there are reasonable grounds for believing—

(a) That there is an organised criminal enterprise; and

(b) That a person who is planning, participating in, or committing, or who has planned, participated in, or committed, such an offence is a member of such an enterprise.]]

Section 312O Privileged evidence—

Where evidence obtained by the interception of a private communication would, but for the interception, have been privileged by virtue of—

(a) Any of the provisions of Part III of the Evidence Amendment Act (No 2) 1980; or

(b) Any rule of law that confers privilege on communications of a professional character between a barrister or solicitor and a client,—

such evidence shall remain privileged and shall not be given in any Court, except with the consent of the person entitled to waive that privilege.

Section 312P Report to be made to Judge on use of warrant or permit—

(1) As soon as practicable after an interception warrant or an emergency permit has expired, the member of the Police who applied for it, or (if that member is unable to act) another commissioned officer of Police, shall make a written report to the Judge who granted the warrant or permit, or (if that Judge is unable to act) to another Judge, on the manner in which the power conferred by the warrant or permit has been exercised and the results obtained by the exercise of that power.

(2) Notwithstanding anything in section 312H of this Act, the Judge who receives a report under subsection (1) of this section shall be entitled to inspect any relevant document held under subsection (1) of that section.

(3) Without limiting the generality of subsection (1) of this section, every report made for the purposes of that subsection shall contain the following information:

(a) Where the listening device was placed:

(b) The number of interceptions made by means of the listening device:

(c) Whether any relevant evidence was obtained by means of the listening device:

(d) Whether any relevant evidence has been, or is intended to be, used in any criminal proceedings:

(e) Whether any records of a private communication intercepted pursuant to the warrant or permit have been destroyed in accordance with section 312I or section 312J of this Act, and, if not, why they have not been destroyed:

(f) Whether the listening device has been retrieved, and, if not, why it has not been retrieved.

(4) On receiving a report under this section, the Judge may require such further information relating to the matter as the Judge thinks fit, and (in addition to any directions the Judge gives for the purposes of section 312J(3) of this Act) the Judge may give such directions as the Judge thinks desirable, whether relating to the retrieval of the listening device, or otherwise.

Section 312Q Commissioner of Police to give information to Parliament—

The Commissioner of Police must include in every annual report prepared by the Commissioner for the purposes of section 65 of the Police Act 1958 the following information in respect of the period under review:

(a) The number of applications for warrants made under section 312B; and

(b) The number of applications for warrants made under section 312CA; and

(c) The number of applications for renewals of warrants made under section 312F; and

(d) The number of applications for emergency permits made under section 312G; and

(e) The number of applications referred to in each of paragraphs (a) to (d) that were granted, and the number that were refused; and

(f) In relation to each of the types of warrant referred to in paragraphs (a) and (b) that were issued,—

(i) The number of warrants that authorised the use of a listening device to intercept the private communications of a named individual:

(ii) The number of warrants that authorised the use of a listening device to intercept private communications at specified premises or a specified place:

(iii) The number of warrants that authorised entry onto private premises; and

(g) The number of occasions on which telephonic communications were intercepted under an emergency permit granted under section 312G; and

(h) The average duration of warrants (including renewals); and

(i) The number of prosecutions that have been instituted in which evidence obtained directly or indirectly from an interception carried out pursuant to a warrant or permit has been adduced, and the result of those prosecutions; and

(j) The number of prosecutions that have been instituted against members of the Police (including former members of the Police where the prosecution relates to behaviour occurring while they were members of the Police) for—

(i) Offences against section 216C (prohibition on disclosure of private communications unlawfully intercepted):

(ii) Offences against section 312K (prohibition on disclosure of private communications lawfully intercepted).]

III MISUSE OF DRUGS AMENDMENT ACT 1978

Section 14 Application by Police for warrant to intercept private communications—

(1) An application may be made in accordance with this section to a Judge of the [High Court] for a warrant for any member of the Police to intercept a private communication by means of a listening device in any case where there are reasonable grounds for believing that—

(a) A person has committed, or is committing, or is about to commit, a drug dealing offence; and

(b) It is unlikely that the Police investigation of the case could be brought to a successful conclusion without the grant of such a warrant.

(2) Every application under subsection (1) of this section shall be made by a commissioned officer of Police, in writing, and on oath, and shall set out the following particulars:

(a) The facts relied upon to show that there are reasonable grounds for believing that a person has committed, or is committing, or is about to commit, a drug dealing offence; and

(b) A description of the manner in which it is proposed to intercept private communications; and

(c) The name and address, if known, of the suspect whose private communications there are reasonable grounds for believing will assist the Police investigation of the case, or, if the name and address of the suspect are not known, a general description of the premises or place in respect of which it is proposed to intercept private communications, being premises or a place believed to be used for any purpose by any person involved in the drug dealing offence; and

(d) The period for which a warrant is requested; and

(e) Whichever of the following is applicable:

(i) The other investigative procedures and techniques that have been tried but have failed to facilitate the successful conclusion of the Police investigation of the case, and the reasons why they have failed in that respect; or

(ii) The reasons why it appears that other investigative procedures and techniques are unlikely to facilitate the successful conclusion of the Police investigation of the case, or are likely to be too dangerous to adopt in the particular case; or

(iii) The reasons why it is considered that the case is so urgent that it would be impractical to carry out the Police investigation using only investigative procedures and techniques other than the interception of private communications.

Section 15 Matters on which Judge must be satisfied in respect of applications—

(1) On an application made to him in accordance with section 14 of this Act, the Judge may grant an interception warrant if he is satisfied that it would be in the best interests of the administration of justice to do so, and that—

(a) There are reasonable grounds for believing that a person has committed, or is committing, or is about to commit a drug dealing offence; and

(b) There are reasonable grounds for believing that evidence relevant to the investigation of the offence will be obtained through the use of a listening device to intercept private communications; and

(c) Whichever of the following is applicable:

(i) Other investigative procedures and techniques have been tried but have failed to facilitate the successful conclusion of the Police investigation of the case; or

(ii) Other investigative procedures and techniques are unlikely to facilitate the successful conclusion of the Police investigation of the case, or are likely to be too dangerous to adopt in the particular case; or

(iii) The case is so urgent that it would be impractical to carry out the Police investigation using only investigative procedures and techniques other than the interception of private communications; and

(d) The private communications to be intercepted are not likely to be privileged in proceedings in a Court of law by virtue of [any of the provisions of Part III of the Evidence Amendment Act (No 2) 1980] or of any rule of law that confers privilege on communications of a professional character between a barrister or solicitor and his client.

[(2) Without limiting subsection (1), in determining whether or not to issue an interception warrant under this section, the Judge must consider the extent to which the privacy of any person or persons would be likely to be interfered with by the interception, under the warrant, of private communications.]

Section 15A Application by Police for warrant to intercept private communications in relation to prescribed cannabis offences—

(1) An application may be made in accordance with this section to a Judge of the High Court for a warrant for any member of the Police to intercept a private communication by means of a listening device in any case where there are reasonable grounds for believing that—

(a) Any member of an organised criminal enterprise is planning, participating in, or committing, or has planned, participated in, or committed, a prescribed cannabis offence; and

(b) The prescribed cannabis offence involves dealing in cannabis on a substantial scale; and

(c) It is unlikely that the Police investigation of the case could be brought to a successful conclusion without the grant of such a warrant.

(2) Every application under subsection (1) must be made by a commissioned officer of Police, in writing, and on oath, and must set out the following particulars:

(a) The facts relied upon to show that there are reasonable grounds for believing that—

(i) There is an organised criminal enterprise; and

(ii) Any member of that enterprise is planning, participating in, or committing, or has planned, participated in, or committed, a prescribed cannabis offence; and

(iii) The prescribed cannabis offence involves dealing in cannabis on a substantial scale; and

(b) A description of the manner in which it is proposed to intercept private communications; and

(c) The name and address, if known, of the suspect whose private communications there are reasonable grounds for believing will assist the Police investigation of the case, or, if the name and address of the suspect are not known, a general description of the premises or place in respect of which it is proposed to intercept private communications, being premises or a place believed to be used for any purpose by any member of the organised criminal enterprise; and

(d) The period for which a warrant is requested; and

(e) Whichever of the following is applicable:

(i) The other investigative procedures and techniques that have been tried but have failed to facilitate the successful conclusion of the Police investigation of the case, and the reasons why they have failed in that respect; or

(ii) The reasons why it appears that other investigative procedures and techniques are unlikely to facilitate the successful conclusion of the Police investigation of the case, or are likely to be too dangerous to adopt in the particular case; or

(iii) The reasons why it is considered that the case is so urgent that it would be impractical to carry out the Police investigation using only investigative procedures and techniques other than the interception of private communications.

Section 15B Matters on which Judge must be satisfied in respect of applications relating to prescribed cannabis offences—

(1) On an application made in accordance with section 15A, the Judge may grant an interception warrant if the Judge is satisfied that it

would be in the best interests of the administration of justice to do so, and that—

(a) There are reasonable grounds for believing that—

(i) There is an organised criminal enterprise; and

(ii) Any member of that enterprise is planning, participating in, or committing, or has planned, participated in, or committed, a prescribed cannabis offence; and

(iii) The prescribed cannabis offence involves dealing in cannabis on a substantial scale; and

(b) There are reasonable grounds for believing that evidence relevant to the investigation of the case will be obtained through the use of a listening device to intercept private communications; and

(c) Whichever of the following is applicable:

(i) Other investigative procedures and techniques have been tried but have failed to facilitate the successful conclusion of the Police investigation of the case; or

(ii) Other investigative procedures and techniques are unlikely to facilitate the successful conclusion of the Police investigation of the case or are likely to be too dangerous to adopt in the particular case; or

(iii) The case is so urgent that it would be impractical to carry out the Police investigation using only investigative procedures and techniques other than the interception of private communications; and

(d) The private communications to be intercepted are not likely to be privileged in proceedings in a court of law by virtue of any of the provisions of Part III of the Evidence Amendment Act (No 2) 1980 or of any rule of law that confers privilege on communications of a professional character between a barrister or solicitor and a client.

(2) Without limiting subsection (1), in determining whether or not to issue an interception warrant under this section, the Judge must consider the extent to which the privacy of any person or persons would be likely to be interfered with by the interception, under the warrant, of private communications.]

Section 16 Contents and term of warrant—

(1) Every interception warrant shall be issued in the [prescribed form], and shall—

(a) State the offence in respect of which the warrant is granted; and

[(b) State,—

(i) In the case of a warrant granted under section 15, the name and address of the suspect, if known, whose private communications may be intercepted, or, where the suspect's name and address are not known, the premises or place in respect of which private communications may be intercepted, being premises or a place believed to be used for

any purpose by any person involved in the drug dealing offence; or

(ii) In the case of a warrant granted under section 15B, the name and address of the suspect, if known, whose private communications may be intercepted, or, where the suspect's name and address are not known, the premises or place in respect of which private communications may be intercepted, being premises or a place believed to be used or any purpose by any member of the organised criminal enterprise; and]

(c) Specify the commissioned officer of Police who (with any other member of the Police or . . . officer of Customs for the time being assisting him) may intercept the private communications; and

(d) Where the Judge considers it necessary, contain express authority to enter (with force, where necessary) any [craft,] carriage, vehicle, or premises, for the purpose of placing, servicing, or retrieving a listening device; and

(e) Contain such additional terms and conditions as the Judge considers advisable in the public interest.

(2) Without limiting subsection (1) of this section, where it is proposed to place a listening device in the residential or business premises of a person who is a barrister or solicitor, or a clergyman, or a registered medical practitioner, the Judge shall prescribe such conditions (if any) as he considers desirable to avoid so far as practicable the interception of communications of a professional character to which the barrister or solicitor or clergyman or registered medical practitioner is a party.

(3) Every interception warrant shall be valid for such period, not exceeding 30 days, as the Judge shall specify in the warrant.

Section 17 Effect of warrant—

Every interception warrant shall have effect, according to its terms, to authorise the interception of private communications by means of a listening device.

Section 18 Renewal of warrants—

(1) Any Judge of the [High Court] may from time to time grant a renewal of an interception warrant upon application made to him at any time before the warrant (or any current renewal thereof) has expired.

(2) Every application for the renewal of an interception warrant shall be made in the manner provided by section 14 [or, as the case requires, section 15A] of this Act, and shall give—

(a) The reason and period for which the renewal is required; and

(b) Full particulars, together with times and dates, of any interceptions made or attempted under the warrant, and an indication of the nature of the information that has been obtained by every such interception.

(3) Every such application shall be supported by such other information as the Judge may require.

(4) A renewal of an interception warrant may be granted under this section if the Judge is satisfied that the circumstances described in section 15 [or, as the case requires, section 15B] of this Act still obtain.

(5) Every renewal of an interception warrant shall be valid for such period, not exceeding 30 days, as the Judge shall specify in the renewal.

(6) A renewal of an interception warrant may be granted upon an application made within the time prescribed by subsection (1) of this section notwithstanding that the warrant (or any renewal thereof) has expired before the application is determined.

(7) Nothing in this section shall prevent a Judge from granting a second or subsequent renewal of an interception warrant upon an application duly made to him.

Section 19 Emergency permits—

(1) In any case where a Judge is satisfied that circumstances exist that would justify the grant of an interception warrant under section 15 [or, as the case requires, section 15B] of this Act, but the urgency of the situation requires that the interception should begin before a warrant could with all practicable diligence be obtained, the Judge may, orally or in writing, grant an emergency permit for the interception of private communications in respect of particular premises or a particular place and in a particular manner.

(2) Repealed

(3) Any application for an emergency permit may be made orally, but otherwise every such application shall comply with the requirements of section 14 [or, as the case requires, section 15A] of this Act.

(4) Where the Judge grants the application for an emergency permit, he shall forthwith make a note in writing of the particulars of the application. The note shall be filed in the [High Court] Registry nearest to where the application is made, and shall, for the purposes of section 20(1) of this Act, be deemed to be a document relating to the

application for the permit. The Judge shall also make a note of the terms of the permit.

(5) The provisions of section 16 of this Act, so far as they are applicable and with the necessary modifications, shall apply to emergency permits in the same manner as they apply to interception warrants.

(6) Every emergency permit shall remain valid for 48 hours from the time when it is given, and shall then expire.

(7) On filing the report required by section 28 of this Act, the member of the Police who applied for the emergency permit (or, if he is not the member filing the report, then that member) may apply to the Judge who granted the permit (or, if he is not the Judge receiving the report, then that Judge) for a certificate confirming the permit pursuant to subsection (9) of this section.

(8) Where the Police, within the period of 48 hours during which the emergency permit is valid, apply for an interception warrant in place of the permit, the member of the Police applying for the warrant may also apply for a certificate confirming the permit pursuant to subsection (9) of this section.

(9) The Judge to whom an application is made pursuant to subsection (7) or subsection (8) of this section shall issue a certificate confirming the permit if he is satisfied, having regard to the requirements of section 15 [or, as the case requires, section 15B] of this Act, that if the original application for the emergency permit had been an application for an interception warrant, he would have granted a warrant.

(10) For the purposes of section 25 of this Act, an interception of a private communication pursuant to an emergency permit shall be deemed to have been made unlawfully unless the Judge to whom an application is made in accordance with subsection (7) or subsection (8) of this section issues a certificate confirming the permit pursuant to subsection (9) of this section.

Section 20 Security of applications—

(1) As soon as an application for an interception warrant or for a renewal of an interception warrant or for an emergency permit or for a certificate confirming an emergency permit has been determined by the Judge, the Registrar shall place all documents relating to the application (except the warrant or renewal or permit or certificate itself) in a packet, seal the packet, and thereafter keep it in safe custody, subject to the succeeding provisions of this section.

(2) Notwithstanding any enactment or rule of law or rules of Court entitling any party to any proceedings to demand the production of any documents, no such party shall be entitled to demand the production of any documents held in safe custody pursuant to subsection (1) of this section, except in accordance with the succeeding provisions of this section.

(3) Every such party who requires the production of any document held in safe custody pursuant to subsection (1) of this section shall, except in a case to which subsection (9) or subsection (10) of this section applies, apply in writing to the Registrar, who shall forthwith notify the senior Police officer in the district.

(4) If, within 3 days after notice is given to the senior Police officer in the district under subsection (3) of this section, that officer gives written notice to the Registrar that he intends to oppose the production of the documents, the Registrar shall refer the matter to a Judge.

(5) Where the senior Police officer in the district does not give written notice to the Registrar as aforesaid, the Registrar shall produce the documents to the party applying for production.

(6) Where a matter is referred to a Judge pursuant to subsection (4) of this section, both the person requesting production of the documents and the member of the Police opposing production shall be given an opportunity to be heard.

(7) If the Judge is satisfied that information in any document the production of which is in dispute identifies or is likely to lead to the identification of a person who gave information to the Police, or of any member of the Police whose identity was concealed for the purpose of any relevant investigation and has not been subsequently revealed, he may, if he believes it in the public interest to do so, order that the whole or any specified part of the document be not produced.

(8) Subject to the provisions of subsection (7) of this section, the judge shall order the production of the documents to the party requesting it.

(9) Where a request for the production of any document kept in safe custody pursuant to subsection (1) of this section is made in the course of any proceedings presided over by a Judge and the request is opposed, the judge shall adjudicate upon the matter as if it had been referred to him pursuant to subsection (4) of this section.

(10) Where such a request is made in the course of any other proceedings, the presiding judicial officer shall forthwith refer the matter to a Judge for adjudication as aforesaid.

(11) Notwithstanding anything in this section, every Judge or [District Court Judge] who is presiding over any proceedings in which the issue of an interception warrant or emergency permit is in issue shall be entitled to inspect any relevant document held under subsection (1) of this section.

Section 21 Destruction of irrelevant records made by use of listening device—

[(1) Every person who intercepts a private communication in pursuance of an interception warrant or any emergency permit must, as soon as practicable after it has been made, destroy any record, whether written or otherwise, of the information obtained by that interception if none of the information directly or indirectly relates to—

(a) The commission of a drug dealing offence or a prescribed cannabis offence; or

(b) The commission of a specified offence or a serious violent offence (as those terms are defined in section 312A of the Crimes Act 1961), or a conspiracy to commit such an offence.]

(2) Every person who fails to comply with subsection (1) of this section commits an offence and is liable on summary conviction to a fine not exceeding $500.

Section 22 Destruction of relevant records made by use of listening device—

[(1) The Commissioner of Police must ensure that every record, whether written or otherwise, of the information obtained by the Police from the interception of a private communication in pursuance of an interception warrant or an emergency permit, being information that relates wholly or partly and directly or indirectly to—

(a) The commission of a drug dealing offence or a prescribed cannabis offence; or

(b) The commission of a specified offence or a serious violent offence (as those terms are defined in section 312A of the Crimes Act 1961), or a conspiracy to commit such an offence,—

is destroyed as soon as it appears that no proceedings, or no further proceedings, will be taken in which the information would be likely to be required to be produced in evidence.]

(2) Nothing in subsection (1) of this section shall apply to—

(a) Any record of any information adduced in proceedings in any Court, or (in any case where the defendant pleads guilty) of any record of any information that, in the opinion of the Judge to whom the report referred to in subsection (3) of this section is made, would have been adduced had the matter come to trial:

(b) Any record of any information contained in any transcript or written statement given to any person in accordance with section 24(a) of this Act.

(3) Every report made to a Judge in accordance with section 28 of this Act shall state whether or not subsection (1) of this section has yet been complied with, and, if it has not, the Judge shall give such directions relating to the eventual destruction of the record as he thinks necessary to ensure compliance with that subsection, including a requirement that he be advised when the record has been destroyed.

Section 23 Prohibition on disclosure of private communications lawfully intercepted—

(1) No person who—

(a) Intercepts or assists in the interception of a private communication in pursuance of an interception warrant or emergency permit; or

(b) Acquires knowledge of a private communication as a direct or indirect result of that interception—

shall knowingly disclose the substance, meaning, or purport of that communication, or any part of that communication, otherwise than in the performance of his duty.

(2) Every person who acts in contravention of subsection (1) of this section commits an offence and is liable on summary conviction to a fine not exceeding $500.

Section 24 Notice to be given of intention to produce evidence of private communication—

Particulars of a private communication intercepted pursuant to an interception warrant or an emergency permit shall not be received in evidence by any Court against any person unless the party intending to adduce it has given to that person reasonable notice of his intention to do so, together with—

(a) A transcript of the private communication where he intends to adduce it in the form of a recording, or a written statement setting forth the full particulars of the private communication where he intends to adduce oral evidence of it; and

(b) A statement of the time, place, and date of the private communication, and of the names and addresses of the parties to the communication, if they are known.

Section 25 Inadmissibility of evidence of private communications unlawfully intercepted—

(1) Subject to subsections (2) [to (4)] of this section, where a private communication intercepted by means of a listening device otherwise than in pursuance of an interception warrant or emergency

permit issued under this Act or of any authority conferred by or under any other enactment has come to the knowledge of a person as a direct or indirect result of that interception or its disclosure, no evidence [so acquired] of that communication, or of its substance, meaning, or purport, and no [other] evidence obtained as a direct or indirect result of the interception or disclosure of that communication, shall be given against any person, except in proceedings relating to the unlawful interception of a private communication by means of a listening device or the unlawful disclosure of a private communication unlawfully intercepted in that manner.

[(2) Even though certain evidence is inadmissible in criminal proceedings by virtue of subsection (1), a Court may admit that evidence if the following conditions are satisfied:

(a) The proceedings are for—

(i) A drug dealing offence; or

(ii) A prescribed cannabis offence; and

(b) The evidence is relevant; and

(c) The evidence is inadmissible by virtue of subsection (1) merely because of a defect in form, or an irregularity in procedure, in—

(i) The application for or the granting of the interception warrant or emergency permit; or

(ii) The manner in which the evidence was obtained; and

(d) The defect in form or irregularity in procedure—

(i) Was not substantive; and

(ii) Was not the result of bad faith.]

(3) Subsection (1) of this section shall not render inadmissible against any party to a private communication evidence of that communication that has, in the manner referred to in that subsection, come to the knowledge of the person called to give evidence, if all the parties to the communication consent to that person giving the evidence.

[(4) Subsection (1) of this section shall not render inadmissible evidence of a private communication by any person who intercepted that communication by means of a listening device with the prior consent of any party to the communication.]

Section 26 Inadmissibility of evidence of private communications lawfully intercepted—

(1) Where a private communication intercepted in pursuance of an interception warrant or an emergency permit discloses evidence relating to any offence other than a drug dealing offence [or a prescribed cannabis offence], no evidence of that communication, or of its substance, meaning, or purport, shall be given in any Court.

[(2) If, in any proceedings for [a specified offence or a serious violent offence (as those terms are defined in section 312A of the Crimes Act 1961)] or a conspiracy to commit such an offence,—

(a) Evidence is sought to be adduced of a private communication intercepted in pursuance of an interception warrant or an emergency permit issued under this Part of this Act; and

(b) The Judge is satisfied, on the evidence then before the Judge,—

(i) That a warrant or permit could have been issued under Part XIA of the Crimes Act 1961; and

(ii) That the evidence sought to be adduced would have been admissible if the warrant or permit had been issued under that Part of that Act,—

the evidence may be admitted notwithstanding subsection (1) of this section.]

[(3) Subsection (4) applies where,—

(a) In any proceedings for a specified offence (as so defined), a Judge has to decide whether or not evidence relating to the offence can be admitted under subsection (2); and

(b) In order to make that decision, the Judge has to decide the issue of whether or not a warrant or permit could have been issued under Part XIA of the Crimes Act 1961 in respect of the specified offence.

[(4) Where this subsection applies, the Judge must decide the issue referred to in subsection (3)(b) as if a warrant or permit could be issued under section 312C or section 312G of the Crimes Act 1961 in respect of a specified offence regardless of whether or not there are reasonable grounds for believing—

(a) That there is an organised criminal enterprise; and

(b) That a person who is planning, participating in, or committing, or who has planned, participated in, or committed, such an offence is a member of such an enterprise; and

(c) That such an offence is part of a continuing course of criminal conduct planned, organised, or undertaken by members of such an enterprise.]

Section 27 Privileged evidence—

Where evidence obtained by the interception of a private communication would, but for the interception, have been privileged by virtue of—

[(a) Any of the provisions of Part III of the Evidence Amendment Act (No 2) 1980; or]

(b) Any rule of law that confers privilege on communications of a professional character between a barrister or solicitor and his client,—

such evidence shall remain privileged and shall not be given in any Court, except with the consent of the person entitled to waive that privilege.

Section 28 Report to be made to Judge on use of warrant or permit—

(1) As soon as practicable after an interception warrant or an emergency permit has expired, the member of the Police who applied for it, or (if he is unable to act) another commissioned officer of Police, shall make a written report to the Judge who granted the warrant or permit, or (if he is unable to act) to another Judge, on the manner in which the power conferred by the warrant or permit has been exercised and the results obtained by the exercise of that power.

(2) Notwithstanding anything in section 20 of this Act, the Judge who receives a report under subsection (1) of this section shall be entitled to inspect any relevant document held under subsection (1) of that section.

(3) Without limiting the generality of subsection (1) of this section, every report made for the purposes of that subsection shall contain the following information:

(a) Where the listening device was placed:

(b) The number of interceptions made by means of the listening device:

(c) Whether any relevant evidence was obtained by means of the listening device:

(d) Whether any relevant evidence has been, or is intended to be, used in any criminal proceedings:

(e) Whether any records of a private communication intercepted pursuant to the warrant or permit have been destroyed in accordance with section 21 or section 22 of this Act, and, if not, why they have not been destroyed:

(f) Whether the listening device has been retrieved, and, if not, why it has not been retrieved.

(4) On receiving a report under this section, the Judge may require such further information relating to the matter as he thinks fit, and (in addition to any directions he gives for the purposes of section 22(3) of this Act) he may give such directions as he thinks desirable, whether relating to the retrieval of the listening device, or otherwise.

Section 29 Commissioner of Police to give information to Parliament—

The Commissioner of Police must include in every annual report prepared by the Commissioner for the purposes of section 65 of the Police Act 1958 the following information in respect of the period under review:

(a) The number of applications for warrants made under section 14; and

(b) The number of applications for warrants made under section 15A; and

(c) The number of applications for renewals of warrants made under section 18; and

(d) The number of applications for emergency permits made under section 19; and

(e) The number of applications referred to in each of paragraphs (a) to (d) that were granted, and the number that were refused; and

(f) In relation to each of the types of warrant referred to in paragraphs (a) and (b) that were issued,—

(i) The number of warrants that authorised the use of a listening device to intercept the private communications of a named individual:

(ii) The number of warrants that authorised the use of a listening device to intercept private communications at specified premises or a specified place:

(iii) The number of warrants that authorised entry onto private premises; and

(g) The number of occasions on which telephonic communications were intercepted under an emergency permit granted under section 19; and

(h) The average duration of warrants (including renewals); and

(i) The number of prosecutions that have been instituted in which evidence obtained directly or indirectly from an interception carried out pursuant to a warrant or permit has been adduced, and the result of those prosecutions; and

(j) The number of prosecutions that have been instituted against members of the Police (including former members of the Police where the prosecution relates to behaviour occurring while they were members of the Police) for offences against section 23 (prohibition on disclosure of private communications lawfully intercepted).]

IV TELECOMMUNICATIONS ACT 1987

Section 10A Application for call data warrant—

(1) Any member of the Police or any Customs officer may apply to a District Court Judge for the issue of a call data warrant.

(2) An application must be made in writing and on oath.

Section 10B Issue of call data warrant—

(1) On an application made under section 10A, a District Court Judge may issue a warrant under this section if he or she is satisfied that there is reasonable ground for believing—

(a) That an offence punishable by imprisonment has been, or is being, or is likely to be committed; and

(b) That evidence relevant to the investigation of the offence will be obtained—

(i) By the use of a telephone analyser; or

(ii) From call associated data provided by a network operator.

(2) A District Court Judge may issue a warrant under this section—

(a) In respect of a person who is suspected of having committed, or of committing, or of being likely to commit, the offence to which the warrant relates; or

(b) In respect of someone other than the suspected offender, in any case where obtaining call associated data in respect of that person may lead to the identification of the suspected offender.

(3) A warrant issued under this section must comply with the requirements of section 10I.

Section 10C Effect of warrant—

(1) A call data warrant authorises any member of the Police or (as the case requires) any Customs officer to do the following things:

(a) To connect a telephone analyser, or to have a telephone analyser connected, to any part of a network, or to any line, apparatus, or equipment connected to any part of a network, that is used, or (where applicable) is suspected of being used, by the person named in the warrant:

(b) To monitor the telephone analyser, or to have the telephone analyser monitored:

(c) To require the network operator whose network is subject to the warrant to supply, to a member of the Police or (as the case requires) a Customs officer, call associated data in respect of the person named in the warrant.

(2) Where subsection (1)(c) applies, and for as long as the warrant remains in force, the network operator must supply the call associated data—

(a) At such intervals, or at such times; and

(b) In such manner, or in such form, or both,—

as the member of the Police or (as the case requires) the Customs officer requires.

(3) Before requiring a network operator to supply call associated data under subsection (1)(c), the member of the Police or (as the case requires) the Customs officer must consult with the network operator to ensure that compliance with the terms of the requirement will not unreasonably interfere with the normal operation of the operator's network.

(4) Except as provided in section 10D, a call data warrant does not authorise any person to enter any premises or place without the consent of the owner or occupier of those premises or that place.

Section 10D Network operator required to assist in execution of warrant—

A network operator that owns or operates a network that is subject to a call data warrant must provide such assistance as is necessary to enable any person who is authorised by the warrant to connect a telephone analyser—

(a) To locate the part of the network to which the analyser is to be connected (including, where necessary, any relevant line, apparatus, or equipment); and

(b) To connect the analyser in accordance with the warrant.

Section 10E Failure to comply with call data warrant—

Every network operator commits an offence and is liable on summary conviction to a fine not exceeding $2,000 who,—

(a) Fails, without reasonable excuse, to comply with the requirements of section 10D; or

(b) Having been required under a call data warrant to supply call associated data,—

(i) Fails, without reasonable excuse, to comply with that requirement (including any requirement imposed under section 10C(2)); or

(ii) Knowingly supplies information that is false or misleading in purported compliance with that requirement.

Section 10F Telephone analysers must comply with technical requirements—

(1) A telephone analyser must not be connected under a call data warrant to any part of a network unless—

(a) The analyser is approved (or is of a kind approved) for connection to that network by the network operator that owns or operates the network; and

(b) The analyser is connected to the network in the manner (if any) approved by that network operator.

(2) A network operator may—

(a) Refuse to approve a telephone analyser or a kind of telephone analyser for the purposes of subsection (1)(a); or

(b) Determine the manner in which telephone analysers are connected to the operator's network for the purposes of subsection (1)(b)—

only if it is necessary, and only to the extent necessary, to prevent interference with or damage to the network.

Section 10G Existence of call data warrant not to be disclosed—

(1) A network operator whose network is, or has been, subject to a call data warrant must not disclose the existence or operation of the warrant to any person except—

(a) The Commissioner of Police or a member of the Police who is authorised by the Commissioner to receive the information; or

(b) The Comptroller of Customs or a Customs officer who is authorised by the Comptroller to receive the information; or

(c) An employee or agent of the network operator, for the purpose of ensuring compliance with the warrant; or

(d) A lawyer, for the purpose of obtaining legal advice or representation in relation to the warrant.

(2) A person referred to in paragraph (a) or paragraph (b) of subsection (1) to whom disclosure of the existence or operation of a call data warrant has been made must not disclose the existence or operation of the warrant except to another person of the kind referred to in that subsection, for the purpose of the performance of the first-mentioned person's duties.

(3) A person referred to in paragraph (c) of subsection (1) to whom disclosure of the existence or operation of a call data warrant has been made must not disclose the existence or operation of the warrant except to another person of the kind referred to in that subsection, for the purpose of ensuring that the warrant is complied with or obtaining legal advice or representation in relation to the warrant.

(4) A person referred to in paragraph (d) of subsection (1) to whom disclosure of the existence or operation of a call data warrant has been made must not disclose the existence or operation of the warrant except to a person of the kind referred to in that subsection, for the purpose of giving legal advice or making representations in relation to the warrant.

(5) Nothing in subsections (1) to (4) prevents the disclosure of the existence or operation of a call data warrant—

(a) In connection with, or in the course of, proceedings before a court; or

(b) Under section 10R; or

(c) By the Police or the New Zealand Customs Service, where disclosure is made in response to a request made under the Official Information Act 1982 or the Privacy Act 1993.

Section 10H Offences—

(1) Every person commits an offence who knowingly contravenes any of subsections (1) to (4) of Section 10G.

(2) Every person who commits an offence against subsection (1) is liable on summary conviction,—

(a) In the case of an individual, to a fine not exceeding $2,000:

(b) In the case of a body corporate, to a fine not exceeding $5,000.

(3) Every person commits an offence who discloses any information in contravention of any of subsections (1) to (4) of section 10G, in any case where that person—

(a) Knows that the person is not legally authorised to disclose the information; and

(b) Discloses the information either—

(i) For the purpose of obtaining, directly or indirectly, an advantage or a pecuniary gain for that person or any other person; or

(ii) With intent to prejudice any investigation into the commission or possible commission of any offence.

(4) Every person who commits an offence against subsection (3) is liable on summary conviction,—

(a) In the case of an individual, to imprisonment for a term not exceeding 6 months or a fine not exceeding $5,000:

(b) In the case of a body corporate, to a fine not exceeding $10,000.

Section 10I Form and content of warrant—

(1) A call data warrant must be in the prescribed form.

(2) A call data warrant must be directed—

(a) To members of the Police generally; or

(b) To Customs officers generally.

(3) A call data warrant must contain the following particulars:

(a) The offence or offences in respect of which the warrant is issued:

(b) The kind of telecommunication in respect of which call associated data is authorised to be obtained:

(c) The name and address of the person in respect of whom call associated data is authorised to be obtained:

(d) If known, the telephone number to which the warrant relates:

(e) If that telephone number is not known, the premises or place in respect of which a telephone analyser may be used, being premises or a place used or suspected of being used, by the person to whom the warrant relates, for the purposes of, or for any purpose relating to, an offence in respect of which the warrant is issued:

(f) The period for which the warrant is to be in force.

Section 10J Duration of warrant—

Unless renewed under section 10K, a call data warrant expires at the end of the period (not exceeding 30 days) specified in the warrant.

Section 10K Renewal of warrant—

(1) Any member of the Police or any Customs officer may apply to a District Court Judge for the renewal of a call data warrant that has not expired.

(2) An application for the renewal of a call data warrant must be in writing and on oath.

(3) On an application made under this section, a District Court Judge may renew a call data warrant if he or she is satisfied that the circumstances specified in section 10B(1) still apply.

(4) A call data warrant may be renewed under this section for a period of not more than 30 days.

(5) The period for which a call data warrant is renewed must be endorsed on the warrant, and (unless renewed again) the warrant expires at the end of that period.

(6) A call data warrant may be renewed 1 or more times under this section.

Section 10L Security of applications for warrants—

(1) As soon as a District Court Judge has determined an application for a call data warrant or for the renewal of a call data warrant, all documents relating to the application (except the warrant itself) must be dealt with in accordance with subsection (2).

(2) Where this section applies, the Registrar of the relevant District Court must—

(a) Place the documents in a packet; and

(b) Seal the packet; and

(c) Keep the packet in safe custody, subject to sections 10M to 10Q.

Section 10M Restriction on production of documents relating to application—

(1) Regardless of any enactment or rule of law or any rules of court entitling any party to any proceedings to demand the production of any documents, no such party is entitled to demand the production of any documents held in safe custody under section 10L.

(2) Subsection (1) is subject to sections 10N to 10Q.

Section 10N Application for production of documents—

(1) Any party to any proceedings who requires the production of any document held in safe custody under section 10L must (except in a case to which section 10P applies) apply in writing to the Registrar who holds the document.

(2) On receiving notification under subsection (1), the Registrar must, without delay, notify—

(a) The senior Police officer in the district, in any case where the document is or relates to an application for a call data warrant sought by a member of the Police:

(b) The senior Customs officer in the district, in any case where the document is or relates to an application for a call data warrant sought by a Customs officer.

(3) If, within 3 days after notice is given under subsection (2), the officer to whom the notice is given notifies the Registrar in writing that the officer intends to oppose the production of the document, the Registrar must refer the application for production to a District Court Judge.

(4) Where the officer does not notify his or her opposition to the Registrar within the period specified in subsection (3), the Registrar must produce the document to the party applying for production.

Section 10O Application referred to Judge—

(1) If, under section 10N(3), a Registrar refers an application for production to a District Court Judge, the application must be dealt with in accordance with this section.

(2) Both the person applying for production of the document and the member of the Police or Customs officer opposing production must be given an opportunity to be heard.

(3) If the District Court Judge is satisfied that information in any document whose production is sought identifies, or is likely to lead to the identification of,—

(a) A person who gave information to the Police, or to the New Zealand Customs Service; or

(b) Any member of the Police, or any Customs officer, whose identity was concealed for the purpose of any relevant investigation and has not been subsequently revealed,—

the Judge may, if the Judge believes it in the public interest to do so, order that the whole or any specified part of the document not be produced.

(4) If the Judge does not make an order under subsection (3), the Judge must order the production of the document to the party requesting it.

Section 10P Request for production made in course of proceedings—

(1) If—

(a) A request for the production of any document kept in safe custody under section 10L is made in the course of any proceedings presided over by a District Court Judge or a Judge of the High Court; and

(b) The request is opposed,—

that Judge must adjudicate on the matter as if it had been referred under section 10N(3) to a District Court Judge, and section 10O applies accordingly with any necessary modifications.

(2) If—

(a) A request for the production of any document kept in safe custody under section 10L is made in the course of any other proceedings; and

(b) The request is opposed,—

the presiding judicial officer must, without delay, refer the matter to a District Court Judge for adjudication under section 10O.

Section 10Q Judge entitled to inspect any relevant document—

Regardless of anything in any of sections 10L to 10P, any Judge who is presiding over any proceedings in which the issue of a call data warrant is in issue is entitled to inspect any relevant document held under section 10L.

Section 10R Reports to Parliament on call data warrants—

(1) The Commissioner of Police must include in every annual report prepared by the Commissioner for the purposes of section 65 of the Police Act 1958 the following information in respect of the period under review:

(a) The number of applications made by members of the Police for call data warrants:

(b) The number of applications made under section 10K by members of the Police for renewals of call data warrants:

(c) The number of applications referred to in each of paragraphs (a) and (b) that were granted, and the number that were refused:

(d) The average duration of call data warrants (including renewals) issued to members of the Police.

(2) The Comptroller of Customs must include in his or her annual report under section 30 of the State Sector Act 1988 the following information in respect of the period under review:

(a) The number of applications made by Customs officers for call data warrants:

(b) The number of applications made under section 10K by Customs officers for renewals of call data warrants:

(c) The number of applications referred to in each of paragraphs (a) and (b) that were granted, and the number that were refused:

(d) The average duration of call data warrants (including renewals) issued to Customs officers.

Section 10S Regulations—

The Governor-General may from time to time, by Order in Council, make regulations prescribing the form of call data warrants.]

V NEW ZEALAND BILL OF RIGHTS ACT 1990

Section 5 Justified limitations

Subject to section 4 of this Bill of Rights, the rights and freedoms contained in this Bill of Rights may be subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.

Section 14 Freedom of expression

Everyone has the right to freedom of expression, including the freedom to seek, receive, and impart information and opinions of any kind in any form.

Section 21 Unreasonable search and seizure

Everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise.

VI SUMMARY PROCEEDINGS ACT 1957

Section 2 Interpretation

"Representative", in relation to a corporation, means a person duly appointed by the corporation to represent it for the purpose of doing any act or thing which the representative of a corporation is by this Act authorised to do, but a person so appointed shall not, by virtue only of being so appointed, be qualified to act on behalf of the corporation before the Court for any other purpose:

Section 198 Search warrants—

(1) Any [District Court Judge] or Justice [or Community Magistrate], or any Registrar (not being a constable), who, on an application in writing made on oath, is satisfied that there is reasonable ground for believing that there is in any building, aircraft, ship, carriage, vehicle, box, receptacle, premises, or place—

(a) Any thing upon or in respect of which any offence punishable by imprisonment has been or is suspected of having been committed; or

(b) Any thing which there is reasonable ground to believe will be evidence as to the commission of any such offence; or

(c) Any thing which there is reasonable ground to believe is intended to be used for the purpose of committing any such offence—

may issue a search warrant in the prescribed form.

(2) Every search warrant shall be directed either to any constable by name or generally to every constable. Any search warrant may be executed by any constable.

(3) Every search warrant to search any building, aircraft, ship, carriage, vehicle, premises, or place shall authorise any constable at any time or times within one month from the date thereof to enter and search the building, aircraft, ship, carriage, vehicle, premises, or place with such assistants as may be necessary, and, if necessary, to use force for making entry, whether by breaking open doors or otherwise; and shall authorise any constable to break open any box or receptacle therein or thereon, by force if necessary.

(4) Every search warrant to search any box or receptacle shall authorise any constable to break open the box or receptacle, by force if necessary.

(5) Every search warrant shall authorise any constable to seize any thing referred to in subsection (1) of this section.

(6) In any case where it seems proper to him to do so, the [District Court Judge], Justice, [Community Magistrate,] or Registrar may issue a search warrant on an application made on oath orally, but in that event he shall make a note in writing of the grounds of the application.

(7) Every search warrant may be executed at any time by day or by night.

(8) It is the duty of every one executing any search warrant to have it with him and to produce it if required to do so.

BIBLIOGRAPHY

Australasian Police Commissioners Electronic Crime Steering Committee 2001-2003 *Electronic Crime Strategy of the Police Commissioners' Conference* (Australasian Centre for Policing Research, 2001, Marden, South Australia).

Barnes, Eamonn M, and Burrows, Thomas N "Brief Summary of the Findings of Working Group I of the International Association of Prosecutors" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999) <http://www.stop-childpornog.at/pa_barnes2.html> (last accessed 3 May 2001).

Boss, Amelia H "Tearing Down Paper Barriers" (14 February 2000) *Legal Times* United States <http://www5.law.com/dc-shl/display.cfm?id=2732> (last visited 18 June 2001).

Bruggeman, Willy "Europol" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999) <http://www.stop-childpornog.at/pa_bruggeman.html> (last accessed 3 May 2001).

"Checksum" Webopedia <http://www.webopedia.com/TERM/c/checksum.html> (last accessed 18 June 2001).

Commission of the European Communities *Communication from the Commission to the Council, The European Parliament, The Economic and Social Committee and The Committee of the Regions: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime* (Brussels, 2000).

Committee of Inquiry into Pornography *Pornography: Report of the Ministerial Committee of Inquiry into Pornography* (Department of Justice, Wellington, 1989).

Conclusions and Recommendations of the International Conference 'Combating Child Pornography on the Internet'" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999) <http://www.stop-childpornog.at/pa_kind.html> (last accessed 3 May 2001).

Council of Europe Committee of Ministers *Recommendation No R(91)11 of the Committee of Ministers to Member States Concerning Sexual Exploitation, Pornography, and Prostitution of, and Trafficking in, Children and Young Adults* (Brussels, 1991).

Council of Europe Committee of Ministers *Recommendation No R(95)13 of the Committee of Ministers to Member States Concerning*

Criminal Procedural Law Connected with Information Technology Brussels, 1995).

Council of Europe *Draft Convention on Cyber-Crime (Draft 25)* (Strasbourg, 2000) <http://convetnions.coe.int/treaty/EN/projects/cybercrime25.htm> (last accessed 14 May 2001).

"Declaration" (Sexual Abuse of Children, Child Pornography and Paedophilia on the Internet: An International Challenge – Expert Meeting, UNESCO, Paris, 18-19 January) <http://www.unesco.org/webworld/child_screen/conf_index.html> (last accessed 3 May 2001).

Department of Internal Affairs *Briefing to the Minister of Internal Affairs: November 2000* (Wellington, 2000).

Department of Internal Affairs *Censorship and the Internet* (Wellington, 2001) <http://www.censorship.dia.govt.nz/DIAwebsite.nsf/c7ad5e032528c34c4c2566690076db9b/df667ab0dc96f927cc2568f7007cb1d1!OpenDocument> (last accessed 20 June 2001).

Dworkin, Andrea "Pornography and male supremacy" *Letters from a War Zone* (Secker and Warburg, London, 1988).

European Commission "Background Paper" Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999) <http://www.stop-childpornog.at/pa_eu.html> (last accessed 3 May 2001).

Forman Pollack, Robyn "Creating the Standards of a Global Community: Regulating Pornography on the Internet – An International Concern" (1996) 10 Temp Int'l & Comp LJ 467.

Fournier de Saint Maur, Agnès "The Sexual Abuse of Children via the Internet: a New Challenge for Interpol" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999) <http://www.stop-childpornog.at/ab_maur.asp> (last accessed 3 May 2001).

Government Administration Select Committee "The Terms of Reference of the Inquiry of the Government Administration Committee into the Operation of the Films, Videos, and Publications Classification Act 1993 and Related Issues" (Wellington, 2001) <http://www.clerk.parliament.govt.nz/publications/GAtor.htm> (last accessed 13 June 2001).

Kind, Holger "Combating Child Pornography on the Internet by the German Federal Criminal Police Office" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999)

<http://www.stop-childpornog.at/pa_kind.html> (last accessed 3 May 2001).

MacGillavry, Edwin C "Internet Service Providers and Criminal Investigation" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999) <http://www.stop-childpornog.at/pa_gillavry.html> (last accessed 3 May 2001).

O'Grady, Ron "Opening Address" (Child Pornography on the Internet Experts Meeting, Lyon, 28 May 1998) <http://www.ecpat.net/Childporn/Ron's.html> (last accessed 14 May 2001).

"Paedophiles jailed for porn ring" (13 February 2001) *BBC News Online* United Kingdom <http://news.bbc.co.uk/hi/english/uk/newsid_1168000/1168112.stm> (last accessed on 20 May 2001).

"Porn Ring 'was Real Child Abuse'" <http://news.bbc.co.uk/hi/english/uk/newsid_1109000/1109787.stm> (last accessed 3 May 2001) and "Paedophiles Jailed for Porn Ring" <http://news.bbc.co.uk/hi/english/uk/newsid_1168000/1168112.stm> (last accessed 3 May 2001).

Sieber, Ulrich *Criminal Law Provisions against Child Pornography: A Legal Comparative Study for the Creation of Worldwide Minimum Standards* (German Federal Ministry of Justice, Bonn, 1999).

Taylor, Max "The Nature and Dimensions of Child Pornography on the Internet" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999) <http://www.stop-childpornog.at/pa_taylor.html> (last accessed 3 May 2001).

Wood, Alexander "National Crime Squad, United Kingdom - Briefing Note" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999) <http://www.stop-childpornog.at/ab_maur.asp> (last accessed 3 May 2001).

(last accessed 3 May

rs and Criminal
the Internet, Vienna,
op-childpornog.at/

graphy on the Internet
ww.ecpat.net/
01).

001) *BBC News*
ni/english/uk/
20 May 2001).

s.bbc.co.uk/hi/
accessed 3 May
ttp://news.bbc.co.uk/
st accessed 3 May

Child Pornography: A Legal Comparative Study for the Creation of Worldwide Minimum Standards (German Federal Ministry of Justice, Bonn, 1999).

Taylor, Max "The Nature and Dimensions of Child Pornography on the Internet" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999) <http://www.stop-childpornog.at/pa_taylor.html> (last accessed 3 May 2001).

Wood, Alexander "National Crime Squad, United Kingdom - Briefing Note" (Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999) <http://www.stop-childpornog.at/ab_maur.asp> (last accessed 3 May 2001).