CTRL + ALT + DELETE? CHALLENGES TO NEW ZEALAND CENSORSHIP LAW IN THE INTERNET AGE

BY

LEXIE KIRKCONNELL-KAWANA

A THESIS

SUBMITTED TO THE VICTORIA UNIVERSITY OF WELLINGTON

IN FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE

OF

MASTER OF LAWS

FACULTY OF LAW

TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI

VICTORIA

UNIVERSITY OF WELLINGTON

2016

TABLE OF CONTENTS

Acknowledgements

*To my beautiful family, mum and dad, sister, grandparents, aunties and uncles, cousins and my wahine toa**,** you give me the strength and courage to be better and aim higher. I love you all very much. To James, long may we nit-pick each other's work. To my colleagues and friends, thank you for anointing this journey with wine, tears and laughter. And to Judge Bill Hastings and Dr Petra Butler, your thoughtful guidance and contributions have been invaluable. Thank you for being my champions. Aroha Nui.*

I would also like to extend my thanks to the Office of Film and Literature Classification and the Censorship Compliance Unit for their assistance with this thesis.

Ora, mate,
Hei au koe noho ai.

Abstract

This thesis examines the adequacy of the Films, Videos, and Publications Classification Act 1993 as it applies to expression on the Internet. Weaknesses and inadequacies of the statute are identified and contextualised as flowing from the lack of legal development needed to coincide with the disruptive features of Internet technology, not least the change to the media/content distribution model. The statute is not likely to be fit for purpose as the technology develops further. Three suggestions for reform are proposed which aim to improve the law so that it may withstand future challenges. The reform takes into consideration the purposes of the statute, a normative law-making perspective and the right to freedom of expression. Without adequate censorship legislation, the state risks ceding law-making authority over Internet expression to un-elected, non-democratic and rights-ambivalent private entities.

Word length

The text of this paper (excluding abstract, table of contents, footnotes and bibliography) comprises approximately 48943 words.

Subjects and Topics

Censorship Law
Films, Videos, and Publications Classification Act 1993
The right to freedom of expression
Cyberlaw

I Introduction

Peter Steiner admits that he never knew what the fuss was about when his 1993 cartoon "On the internet, nobody knows you're a dog" rocketed to mass popularity.[1] Although unintended, the simple sketch of an anthropomorphised dog sitting at a computer (presumably presenting itself as a human online) captures the Internet's ubiquity and capacity for connectivity. Additionally, in a more tongue in cheek way, the cartoon captured how the structure of the Internet would enable anonymity and self-expression to flourish unregulated. The cartoon remains resonant to this day, particularly as connecting to the Internet, via personal devices at home, work and in public spaces, is now a formative part of New Zealand life. This enables pervasive expressive activity on such a scale that it is now considered unremarkable. The Internet's unique features extend beyond simply its scale and include its global reach, its ability to enable user-generated expression, and its disruption of the traditional media/content distribution models by which expression is made and made available. This has fundamentally altered the way in which we express ourselves.

The uptake of the Internet in New Zealand is striking, but this follows a familiar pattern of New Zealanders' engagement with expression-facilitating technology. Every time a technology appears—as was the case with film, television, VCR and DVD—New Zealanders are some of its most enthusiastic adopters. But unlike its predecessors, the Internet has a vast multitude of uses that emerge from its core communicative function, which can be harnessed for both beneficial and harmful expressive activity. Mitigating the effect of the harmful expressive activity is one of the seminal challenges for states. This thesis will examine one aspect of this issue in the New Zealand context. It will explore the impact that the Internet has had on New Zealand's censorship law, assess the extent to which this law remains fit for purpose, and propose possible avenues for reform. Specifically it asks what reform would be necessary if the statute is to effectively apply to Internet expression and in a rights-consistent way. This thesis will also address the issue of private censorship and the relationship between private and state censorship and its impact on Internet expression.

Censorship is a long-standing tradition in New Zealand and has been a quotidian affair for the most part, occurring out of sight and out of mind for most New Zealanders. The New Zealand government continues to advocate that the unrestricted public availability of certain expression

[1] Michael Cavna "'Nobody Knows You're a Dog': As iconic Internet cartoon turns 20, creator Peter Steiner knows the idea is as relevant as ever" (Washington Post, July 2013) <https://www.washingtonpost.com/blogs/comic-riffs/post/nobody-knows-youre-a-dog-as-iconic-internet-cartoon-turns-20-creator-peter-steiner-knows-the-joke-rings-as-relevant-as-ever/2013/07/31/73372600-f98d-11e2-8e84-c56731a202fb_blog.html>.

has a likelihood of causing injury to the public good, particularly expression that deals with the subject matter of sex, horror, crime, cruelty and violence.[2] This is not unique to New Zealand. Censorship is a common practice in many comparable countries. Censorship has also progressed to the Internet. But where other countries and other parties (such as online service providers) have developed robust means of censoring the Internet, New Zealand's strategy is comparably more inert.

The Internet has many features that frustrate the state's ability to regulate its citizens' expressive behaviour (discussed in detail in Chapter 3). These include: (a) the fact that expression is globalised, anonymous, interactive and reflexive to the needs of users (and not regulators); (b) the vertical integration of Internet services and platform providers; and (c) the non-linear media/content distribution model. These features certainly pose challenges, but they do not justify the common illusion that the Internet is an open unmoderated public space that is or should be free from censorship. The practice of many comparable states rebuts this, as does the fact that online service and platform providers engage in their own censorship practices, sometimes as conduits for states or in a manner which is endorsed by states. This illusion, combined with misplaced analogies (to pre-Internet forms of communication) frequently used to understand technical aspects of the Internet, has led to poor legal thinking in this area and has resulted in a disproportionate focus being placed on end users as targets of enforcement. The problems with this focus are amplified in a context where the Internet's fragmented and widely-distributed infrastructure undermines the ability of states to (a) intervene and (b) define alternative viable targets of enforcement. With so many dynamics to contend with, regulation can fall short of its purpose.

Censorship legislation is one part of New Zealand's regulatory response to the Internet. The Films, Videos, and Publications Classification Act 1993 (FVPC Act) sets out a classification scheme which empowers independent government bodies to inspect, examine and classify certain expression embodied in "publications". These include the Office of Film and Literature Classification (OFLC), an independent crown entity that examines and classifies publications. Once classified, the publication may be unrestricted, restricted to certain classes of persons (for instance those above a certain age) or banned outright. The subject matter provision of the FVPC Act, s 3(1), limits the scope of the OFLC's reach to only that expression which deals

[2] This reflects a certain view of public morality which will not be appraised in this thesis (there is no room to unpack censorship ethics and theory). State paternalism has been a long-standing tenet of New Zealand censorship and there does not seem to be an appetite to discontinue state censorship based on this rationalisation any time soon, particularly as the OFLC enjoys a high degree of public support, see: http://www.classificationoffice.govt.nz/news/latest-news/research-public-understanding-2016.html.

with sex, horror, crime, cruelty or violence. The expression which is banned includes expression which promotes and supports child sexual exploitation, necrophilia and beastiality. The statute also creates a variety of offences. These offences make criminal certain types of conduct associated with publications, including the making, possession and distribution of certain publications. For instance, a film classified as "objectionable" may not be possessed, exhibited or otherwise supplied or distributed in New Zealand. These offences are then enforced by New Zealand Police, Customs and the Department of Internal Affairs. But this legislation does not create a centralised government authority by which all expression is vetted. Instead, the regulation of expression is much more fractured. For instance, the Broadcasting Act 1989 established a crown entity (the Broadcasting Standards Authority) to oversee television and radio broadcasting standards. Outside of primary legislation there are self-regulatory agencies that deal with print news (the Press Council) and advertising (Advertising Standards Authority). There is no government entity that deals specifically with Internet expression. Internet expression can fall within the remit of the FVPC Act (and relevant publications are classified by the OFLC), however, the legislators that designed the statute lacked foresight regarding the extent of the impact of new technology. Various statutory amendments have not adequately addressed the gaps that have emerged. While the classification scheme is capable of being a meaningful stopgap that prevents injury to the public good flowing from the availability of harmful expression on the Internet, without reform it cannot be fit for purpose.

The most significant constitutional barrier to state censorship of expression (and therefore the most important consideration in any reform) is the right to freedom of expression, codified in the New Zealand Bill of Rights Act 1990 (NZBORA). In order to be justifiable, state censorship must be consistent with NZBORA. No examination of the FVPC Act is complete without due regard to the rights jurisprudence associated with it. As a result, Chapter 2 of this thesis addresses the relationship between the right to freedom of expression and the FVPC Act. Only parts of the classification scheme have been considered and tested by the courts. Debate persists and there is only limited commentary on the scope of the right to freedom of expression and what should be the appropriate rights inquiry when scrutinising the FVPC Act. The courts appear to be satisfied that the scheme overall (as it is) is rights-consistent and/or demonstrably justifiable. Change to the scheme would need to account for this jurisprudence and the finely tuned balancing of the scheme with the right.

This thesis will show, in Chapter 4, that there are several problematic aspects of the FVPC Act which frustrate the statute's application and enforcement in this changing climate (not all of which can be unpacked in the space available). After addressing the theoretical and historical

context that has contributed to the law's development to date, sections of the FVPC Act are appraised: specifically, the definition of "publication" (that is, the means by which the FVPC Act tries to capture expression), and the statutory offences (that is, the sorts of conduct which the statute criminalises). It is argued that poor judicial interpretation has marred the meaning of these statutory provisions and the law is now unclear in many respects. Additionally, there are problems with the way the statute deals with (or does not deal with) the classes of persons who face potential liability and the issue of jurisdiction. It is also argued that a direct fallout of these problems is that enforcement agencies are constrained, limited by the uncertainty of investigating and prosecuting without authority. This in turn creates problems for public and industry compliance.

Such problems are a result of the lack of attention the statute has received in the rapidly changing context of New Zealand's Internet age. When due attention is paid to the legal framework, the obvious questions are: can the uneasy reconciliation of the current classification scheme with the right to freedom of expression persist when applied to Internet expression? What could change to promote both the values of a classification scheme and the justifications that underpin the right to freedom of expression on the Internet? As part of exploring those questions, Chapter 5 examines the relationship between law and norms in the context of the FVPC Act. The law should be not only consistent with rights but also have normative weight. That is, in order to guide behaviour for its intended purpose, the law must be addressed to individual behaviour and not a specific technology, it must be clear who the law addresses and should match up, as closely as possible, to the behaviours and activities which it proposes to regulate.

By way of conclusion, some avenues for reform are proposed in Chapter 6. Specifically, it is suggested that there should be: (a) amendment of certain terms in the statute so that the language may be more certain and intelligible; (b) changes to the enforcement strategy so as to ensure its effectiveness and rights-consistency; and (c) abolition of the current immunity which applies to certain upstream parties (primarily Internet Service Providers). Without any sort of reform, the state will inevitably cede legal authority over censorship (and its vertical rights relationship with citizens) to other jurisdictions or to the private entities that have monopolised the Internet. To avoid this, regulators must address the ways in which the Internet has undermined the adequacy of our current legal framework.

II The state of the right to freedom of expression in New Zealand

Before turning to the challenges posed by the Internet and the adequacy of the current legal framework, it is necessary to frame the discussion by an examination of the right to freedom

of expression, as it is the primary constitutional constraint on state censorship. The right has its own contested theoretical underpinnings, is the subject of ongoing judicial debate and has a unique history with the FVPC Act. This section provides background to the development of the right as it stands with the FVPC Act. This is important context for the discussions concerning the state of the law and the proposals for reform in later sections.

State censorship yields controversy by virtue of its antithetical position to the democratic value of free expression. The FVPC Act did not predate NZBORA, yet within this context of functional rights it is a statute that directly limits the right to freedom of expression. Set out in s 14 of NZBORA, the right states that 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. This does not mean that a person has a right to be given information or that the state is required to make a certain medium available (such as the Internet) but it prima facie prevents the state from restricting a person from receiving information that others can or are willing to impart.[3] While this seems fairly straightforward it is, of course, not so. Geddis describes New Zealand's history with free expression as chequered; the result of a geographically isolated settler society placing a premium upon predictability and conformity.[4] Cheer also notes that common law judges had been making reference to such a principle for some time before its codification.[5] The right's "evolving", "contested" and "contingent" nature means that "it is broadly recognised and respected as a valuable and important social good—until such time as another more valuable or important social good requires that it be restricted".[6]

The classic rationales behind the right include truth-discovery, the maintenance of democracy and individual self-fulfilment.[7] It will be worth returning to some of these justifications later, particularly in relation to whether the Internet promotes these justifications or undermines them. These justifications reflect the Anglo-libertarian tradition of free speech which proposes that state censorship cannot be trusted due to the scope and yield of the state's power, always on the precipice of demagoguery. Critics such as Barendt and Greenawalt are quick to unpack the rationales, questioning their logic and stability in a world where there is "gross inequality

[3] A Butler and P Butler *The New Zealand Bill of Rights Act : a commentary* (2nd ed, LexisNexis NZ, Wellington, 2015) at 13.7.43.

[4] Andrew Geddis "The state of freedom of expression in New Zealand: an admittedly eclectic overview" (2008) 11 Otago L Rev 657 at 658.

[5] Ursula Cheer *Burrows and Cheer Media Law in New Zealand* (7th ed, LexisNexis NZ, Wellington, 2015) at [15.1].

[6] Geddis, above n 4, at 681.

[7] A Butler and P Butler, above n 3, at [13.6].

among communicators", a "control of culture by the privileged", a lack of "objective truth"[8] and where preserving democracy might require the suppression of some speech.[9] The justifications presume citizens are both rational and autonomous. However, this presumption is also criticised: "If some communications are especially likely to lead irrational people to do harmful things, why must the government permit them access to those communications as if they were rational and autonomous, rather than protecting potential victims of their irrational actions?"[10]

The Anglo-libertarian tradition has also not escaped criticism in New Zealand. Tipping J said in *Hosking v Runting*:[11]

> The theory is essentially that it is for the ultimate good of society for citizens to be able to say and publish to others what they want. Liberty is fine in the abstract, but in concrete terms all those living in an organised society must accept some curtailment of their abstract liberty to enjoy freedom of expression when the curtailment is necessary for the greater good of society as a whole and its individual members. Therein lies the conundrum. The liberty theory rests on the ultimate public good; but the full flowering of the theory undoubtedly has the capacity to harm the public good. When the expression in issue provides little public benefit, except in theory, but significant individual or public harm in concrete terms, the theory must give way. Thus, in the particular instance society's pragmatic needs or the welfare of its individual members can outweigh the general benefits supported by the theory of liberty.

The social good of freedom of expression in New Zealand is reflexive, open to and able to tolerate criticism and, most importantly, able to sit with and at times compete with other social goods. These characteristics are reflected in the fact that, despite its statutory codification, New Zealanders' right to freedom of expression is not absolute. The White Paper that preceded the introduction of NZBORA stated that the right is not absolute and must be subject to reasonable limitations, including "censorship by advance" or some vetting of expression by the state.[12] The task for regulators is to ensure that the right is more than merely symbolic (in order to be meaningful to New Zealanders) while addressing speech-related harms (which have been recognised as a consequence of unmoderated speech). Thus its codification in law "should ensure that those responsible for developing and applying the law ask whether an

[8] Kent Greenawalt "Free Speech Justifications" (1989) 89 Columbia Law Review 119 at 131.

[9] Eric Barendt *Freedom of Speech* (2nd ed, Oxford University Press, New York, 2005) at 19.

[10] Greenawalt, above n 8, at 151.

[11] *Hosking v Runting* [2005] 1 NZLR 1 (CA) at [230].

[12] Geoffrey Palmer "A Bill of Rights for New Zealand: A White Paper" [1984–1985] I AJHR A6 at [10.55].

intrusion on freedom of expression is truly justified."[13] It is the justifications used by regulators that must be closely scrutinized. These are the lynchpins that determine the legality of the state's rights-limiting activity such as censorship.

Sections 4, 5 and 6 of NZBORA set out the mechanism for the limitations of rights. They act in concert: s 4 states that other enactments cannot be held "impliedly repealed", "revoked", "invalid" or "ineffective" by the courts for reasons that they are inconsistent with the provisions of NZBORA; s 5 states (subject to s 4) that the rights and freedoms in NZBORA can only be subject to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society; and s 6 stipulates that wherever an enactment can be given a meaning consistent with rights and freedoms, that meaning is to be preferred. Tipping J has said that "New Zealand society as a whole can rightly expect that on appropriate occasions the Courts will indicate whether a particular legislative provision is or is not justified thereunder".[14]

The FVPC Act and NZBORA are in conflict; one endorses free expression while the other endorses censorship. It goes without saying that the classification bodies created by the FVPC Act are subject to the requirements of NZBORA. For instance, OFLC is a crown entity, which brings it directly within the ambit of s 3(a) of the NZBORA.[15] The classification bodies' powers extend to criminalising certain expression and those who seek, receive and impart this expression. When the statute was enacted, the potential for it to be inconsistent with NZBORA was commented upon by the then Attorney-General Paul East, as per his s 7 NZBORA obligation, though only in relation to the strict liability provision of the Bill (s 121):[16]

> In my opinion, imposing retrospective criminal liability without the provision of a defence relating to a lack of knowledge or reasonable belief about the nature of the publication for a simple possession charge cannot be justified by section 5 of the Bill of Rights 1990.

Whilst acknowledging that Parliament could override NZBORA, he recommended that:[17]

---

[13] Cheer, above n 5, at [15.3].

[14] *Moonen v Film and Literature Board of Review* [2000] 2 NZLR 9 (CA) at [20].

[15] Section 3 of NZBORA states: "This Bill of Rights applies only to acts done:
(a) by the legislative, executive, or judicial branches of the Government of New Zealand; or
(b) by any person or body in the performance of any public function, power, or duty conferred or imposed on that person or body by or pursuant to law."

[16] (2 December 1992) Vol 532 NZPD PP 12764.

[17] (2 December 1992) Vol 532 NZPD PP 12765.

> The onus could be shifted to the person in possession of the material, who could be required to show that there was no good ground for believing that the information was objectionable---of course, if it was hard-core pornography, that defence would not get off the ground. I think that would bring the Bill into line with the Bill of Rights 1990.

The recommendations were not implemented, likely because strict liability had been a formative part of censorship legislation since the 20th century and had historical weight.

A Themes from the rights jurisprudence of the FVPC Act

The following is a review of the rights jurisprudence concerning the FVPC Act. It will show that the interpretative exercise is a complex one and uncertainty remains as to how the FVPC Act should be interpreted and applied. The accord struck between the FVPC Act and NZBORA is a delicate one. Any change to the FVPC Act or its application could easily upset this equilibrium. The jurisprudence informs the question of what amounts to protected expression and whether or not the FVPC Act in its rights-limiting capacity is demonstrably justifiable. These questions are revisited later in this thesis, when it turns to possible reform.

(i) The extent of the protection

Free expression has been described as being "as wide as human thought and imagination".[18] The right also purports to protect information and opinions of any kind in any form. However neither of these generalisations clearly signals to individuals whether or not their expressive activity is protected by the right. "Protected" is used in the sense that the government cannot criminalise the individual for their expressive activity, a power available under the FVPC Act. While broad statements have been made by members of the judiciary that, "Censorship of publications to any extent acts as a pro tanto abrogation of the right to freedom of expression"[19] and, "It is their conduct in exercising their censorship role, and so in abridging free speech, which engages the Bill of Rights"[20] the jurisprudence does not leave a robust impression of what protected expression is.

Despite these sentiments, the courts have not said that the FVPC Act or the classification scheme is not justifiable. Of course, rights are not absolute and can be limited. Expression that is justifiably limited does not breach NZBORA. Yet, it is worth considering whether the judicial discourse exposes a certain bias, that some expression is not protected because there was never a right to engage in it in the first place. Thomas J in *Living Word Distributors Ltd v*

---

[18] *Moonen v Film and Literature Board of Review*, above n 14, at [15].

[19] *Moonen v Film and Literature Board of Review*, above n 14, at [15].

[20] *Living Word Distributors Ltd v Human Rights Action Group (Wellington)* [2000] 3 NZLR 570 (CA) at [37].

Human Rights Action Group (Wellington), for instance, did not appear to have a lot of sympathy for the right in the context of the FVPC Act:[21]

> It does not override the objectives of the Act. Nor does it override the statutory direction that the Office of Film and Literary Classification and the Film and Literature Classification Board discharge their respective functions as spelt out in the Act. Section 14 [of NZBORA] is not to be applied in such a way that it erodes the protection Parliament intends the public to have from the publication of pornographic sex or violent material which it perceives to be damaging to the public good. Thus, if in the Board's opinion the publication promotes or supports, or tends to promote or support, the matters contained in subs (2) it must be deemed to be objectionable and s14 can have no bearing on that issue…Freedom of expression does not override or outweigh the express matters contained in subss (2) to (4), but by virtue of its place in the Bill of Rights, it remains a relevant consideration under subs (1) in determining whether the publication is objectionable.

Thomas J appears to suggest that the right can have no bearing once expression is deemed objectionable by the classification body. If this is correct, did the protection of the right ever extend to objectionable expression in the first place? Recent comment from the Supreme Court in *Spark v R* suggests a negative answer. The defendant argued that the definition of the term "publication" needed to be read down in the light of the right to freedom of expression. Echoing Thomas J's judgment, the Court of Appeal had suggested that s 14 was "no defence to" and "no countenance to" the making of objectionable publications.[22] The Supreme Court went on to discuss NZBORA in the following obiter dictum: [23]

> …the offences of creating and possessing publications which are objectionable within s 3(2)(a) of the 1993 Act are clearly aimed at stopping the sexual abuse of children. In such circumstances, the premise that ss 13 or 14 of the New Zealand Bill of Rights Act are engaged at all is highly questionable.

The Supreme Court appears to be suggesting that once a publication is found to be objectionable then either (a) the expression is not protected expression or (b) the legislative purpose (in this case the prevention of sexual exploitation of children) is so clearly a reasonable limitation that the rights inquiry would be superfluous. That the Court showed cynicism towards the fact that s 14 was engaged at all in cases of child sex abuse shows a partiality to

---

[21] *Living Word Distributors Ltd v Human Rights Action Group (Wellington),* above n 20, at [79].

[22] *R v Spark* [2009] NZCA 198 at [13] and [14].

[23] *Spark v R* [2009] NZSC 130, [2010] 1 NZLR 599 at [6].

the proposition that expression about child sex abuse does not fall within the protection of the right.

The current position is that objectionable publications sit outside of the protection of the right. Whether or not the right extends to all human thought and imagination, and information and opinions of any kind in any form, New Zealanders cannot rely on the right as blanket protection from any state censorship of expressive activity.

(ii) What amounts to a reasonable limitation?

When assessing rights-limiting action by the state, s 5 (subject to s 4) states that rights may be subject only to reasonable limits. Following on from s 5, s 6 states that whenever rights-limiting enactments can be given a meaning that is rights-consistent that meaning is to be preferred. The jurisprudence shows that these sections are not necessarily applied sequentially and are not mutually exclusive. There is ongoing debate as to the appropriate methodology which the courts should follow when applying these sections, particularly s 5.

One of the threads of the debate is whether the definitional balancing approach or the ad hoc balancing approach should be adopted. The definitional balancing approach, as described by Huscroft, assumes that "some rights explicitly build questions of evaluation and justification into their definition".[24] This raises the question whether the state ever really has to justify itself when it seeks to limit rights. If a court is simply going to read in-built limitations into rights, this diminishes the burden on the state to justify any potentially rights-infringing conduct.

Conversely, the ad hoc balancing approach is a two stage approach that can be briefly summarized as follows:[25]

> The first stage would be under Part II of NZBORA with a broad definition of rights aimed at detailing the types of government conduct that the courts should be subjecting to detailed scrutiny. The second stage would consist of the assessment of reasonableness of any interference caused by that conduct would occur under s 5 NZBORA.

On this approach, the right is defined broadly and the court is not able to interpret limits or qualifications into the definition of the right. This fosters a "culture of justification" where the onus is not on the individual, who must prove they have a right, but on the state, which must

[24] Grant Huscroft and others *The New Zealand Bill of Rights Act: A Commentary* (Oxford University Press, Australia, 2006) at 52.

[25] Butler and Butler, above n 3, at [4.10.1].

prove the value and importance of the limitation.[26] This is not to say that rights are absolute and cannot ever be limited, but that rights are only capable of being limited by virtue of s 5 NZBORA. Even supposedly self-limiting terms such as "unreasonable" and "peaceful" must be understood broadly by this approach.

In advocating for the definitional balancing approach, Huscroft says that the right to freedom of expression is not a "self-limiting right" but should be defined broadly and that any limitation on the right should be justified under s 5.[27] However, despite this assertion he goes on to contradict himself by arguing that "the right [to freedom of expression] is rendered meaningful only after s 5 is considered". Using perjury as an example, Huscroft suggests that when the perjurer is punished this does not amount to a breach of the right to free expression just because perjury is an act of expression.[28] The right cannot be both broad and without self-limitations but then only meaningful when limited. Rights defined *by* their reasonable limitations are markedly different to rights which are then *subject* to reasonable limitations. The definitional balancing approach must mean that free expression under NZBORA does not protect any and all expression, which is another way of addressing the earlier question of the extent of the protection of the right. Huscroft's definitional balancing approach thus takes a diminished view of what rights protect generally but also diminishes the meaning of ss 4, 5 and 6 of NZBORA and how they apply to rights-limiting activity. For at what point does the self-limiting language end and the state limitation begin? Importantly, on the definitional balancing approach an individual cannot know what these limitations are until the right is defined by the courts and only then whether or not the state has acted contrary to NZBORA.

This debate is reflected in the authorities. In *Moonen v Film and Literature Board of Review*, Tipping J preferred to conflate ss 5 and 6: "It is that meaning which s 6 of the Bill of Rights, aided by s 5, requires the Court to adopt."[29] Joseph confirms that, in some cases, courts do sidestep s 5 entirely and go straight to s 6 or seek out the least rights-constraining interpretation before asking if any resulting limitation is reasonable, but he believes that this bypasses a fundamental tenet of NZBORA.[30] Elias CJ in *Hansen v R*, in contrast to Tipping J, preferred to distinguish between the ordering and purposes of s 5 and s 6, and did not accept that s 6 is

[26] Butler and Butler, above n 3, at [6.9.10].

[27] Huscroft and others, above n 24, at 54.

[28] Huscroft and others, above n 24, at 312 and 54, n 167.

[29] *Moonen v Film and Literature Board of Review*, above n 14, at [17].

[30] Phillip A Joseph (ed) *Constitutional & Administrative Law in New Zealand* (online looseleaf ed, LexisNexis) at [15].

subject to a meaning consistent with limitations justified under s 5.[31] Butler and Butler supplement this proposition by suggesting that "before s 6 of BORA arises for consideration one must first have concluded that without invocation of s 6 of BORA, s 5 of BORA would be offended."[32] This reflects the ad hoc approach: that if the limit is reasonable then there is no need to construe an empowering section restrictively and s 5 need not be "jettisoned".[33]

The first significant case to deal with the issue of whether or not the FVPC Act amounted to a justifiable limitation on the right to free expression was *Moonen v Film and Literature Board of Review* (*Moonen 1*). The appellant challenged the Board of Review's interpretation and application of s 3 of the FVPC Act, asserting that it amounted to an unjustifiable limitation on his right to freedom of expression.[34] It is from this decision that the frequently quoted reference to free expression being "as wide as human thought and imagination" is found. However the Court was quick to establish that there was a threshold by which the right could be limited. Tipping J set out a five step test. The test, as noted by some authors, is simply a reordered restatement of the *Oakes*/proportionality test: a way of modelling how s 4, 5 and 6 of NZBORA should be applied to enactments that are prima facie inconsistent with rights.[35] This test was applied as follows:[36]

> [26] The Board's decision contains no discussion and no reasons why it saw the Book as "promoting" the exploitation of children or young persons for sexual purposes. Reasons are required under s55(1)(c) of the Act. Nor does the Board's decision contain any discussion of the meaning which the Board gave to the concept of promotion.
> [27] In considering the correct meaning of the words "promotes or supports", a Bill of Rights consistent approach is required. It is inevitable in a censorship context that some limit will be placed on freedom of expression, but the combined effect of ss5 and 6 of the Bill of Rights results in a need to put on the words "promotes or supports" such available meaning as impinges as little as possible on freedom of expression.

The effect of this was to read down the meaning of the phrase "promotes and supports" found in s 3(2) of the FVPC Act. Certainly reading down the scope of a rights-limiting provision is one way of making a provision rights consistent, however the Court did not discuss what

---

[31] *Hansen v R* [2007] NZSC 7, [2007] 3 NZLR 1 at [15].

[32] Butler and Butler, above n 3, [6.14.2].

[33] Joseph, above n 30, at [9].

[34] The Film and Literature Board of Review is an independent appeal body that reviews publications that have been classified by the Office of Film and Literature Classification.

[35] Huscroft and others, above n 24, at 184.

[36] Above n 14.

characteristics made the Board of Review's interpretation of s 3(2) inconsistent with the right, simply that the combined effect of ss 5 and 6 would engineer what was necessary to justify the continued rights-consistent application of s 3(2) of the FVPC Act. Presumably, the Court believed that more than one possible meaning of "promotes and supports" was available, and one of the possible meanings was a reasonable limitation on the right whilst the others were not. It is worth noting that the Court in *Hansen* suggested that the *Moonen 1* approach may be a good one to adopt where the meaning of terms was "elastic" and where it was "difficult to determine where Parliament intended the meaning to fall on the continuum".[37] Without reading too much into the comment, it does appear to give greater import to s 6 than s 5. This proposition is supported by the fact that the Court did not discuss what factors were relevant to the consideration of what constituted a reasonable limitation.

The question of what amounts to a reasonable limitation was addressed by the courts in the later decision of *Moonen 2*.[38] The Court qualified Tipping J's statement that limitations on the right must pose "as little interference as possible". It suggested this was counterproductive to the exercise of s 5:[39]

> In essence, a Bill of Rights consistent interpretation is one which involves the least possible reasonable limitation on a Bill of Rights right or freedom, rather than the least possible limitation.

Injecting this *reasonable* qualification may suggest that the threshold which the state must meet to "justify" its infringing action is not high, and may reflect the fact that even if the rights-limiting activity is not justifiable, s 4 would tolerate it regardless. The Court of Appeal found that there was no error of law and that this time the Board of Review had apparently applied the FVPC Act correctly (in a demonstrably justifiable way) and so the appeal was dismissed. The Court did not specify what was different about this Board's application or why it was reasonable. Some note that the outcome overall was surprising given that s 3(2) of the FVPC Act so clearly abrogates the right to freedom of expression.[40]

There continued to be a lack of comment on what made the application of the FVPC Act demonstrably justifiable or not. The Court of Appeal in *Living Word* found that the Board of Review and the lower court had erred in their interpretation of s 3(1), suggesting instead that

---

[37] *Hansen v R*, above n 31, at [94].

[38] *Moonen v Film and Literature Board of Review* [2002] 2 NZLR 754 (CA).

[39] At [12].

[40] Huscroft and others, above n 24, at 329.

"[t]he subject-matter provision is obviously designed as imposing an immediate limitation on the reach of the censorship laws".[41] The Court, similarly to its predecessors, read down the meaning of s 3(1) as this "would accord with s 6 of the Bill of Rights and provide a reasonable limit as can be demonstrably justified in a free and democratic society".[42] Nothing more was said on what amounts to a reasonable limit.

The current position is that the courts appear happy to conflate ss 5 and 6. McLean takes a pessimistic view of the results of the jurisprudence and its practical effect:[43]

> The very purpose of the Board [of Review] is to limit freedom of expression. Any constitutional limits on its powers go to the very core of its jurisdiction and do not merely "grab" occasionally on a particular exercise of statutory discretion. Of course, a court might take the view that having the Board at all is inconsistent with freedom of expression, but it would be unable under the New Zealand Bill of Rights to strike down the legislation giving an independent body the power to limit expression.

What McLean alludes to is that conflating ss 5 and 6 shirks the issue of first deciding whether or not the application of the FVPC Act amounts to a justifiable limitation. To extrapolate further, the lack of guidance as to what does or does not amount to a justifiable limitation creates challenges for the task of determining whether rights are defined by their reasonable limitations or are to be understood broadly and then subject to reasonable limitations.

The way classification bodies now apply ss 3(1) and 3(2) has been anointed by the courts as rights-compliant but there are plenty of other provisions in the statute that are potentially elastic. "Read these narrowly" appears to be the direction of the courts. But not too narrowly. Application of the statute involves not the least possible but the least possible reasonable limitation on the right, in order to be rights-consistent. Unfortunately for individuals trying to make law-abiding expressive choices, the jurisprudence does not leave a robust impression on when the application of the FVPC Act will be demonstrably justifiable and when it will not be (amounting to a rights breach) and therefore if their expressive activity is protected by the right or not.

(iii) Institutional discretion

---

[41] *Living Word Distributors Ltd v Human Rights Action Group (Wellington)*, above n 20, at [30].

[42] At [39].

[43] Janet McLean "The Impact of the Bill of Rights on Administrative Law Revisited: Rights, Utility, and Administration" [2008] NZ L Rev 377 at 396.

The lack of comment by the courts means that it is the classification bodies themselves that must use their discretion when making assessments as to the rights-consistency of applying the FVPC Act. A prescriptive methodology set out by the courts would have obviated this need. However, the courts have repeatedly refused to be more precise than Tipping J's methodology. The Court of Appeal in *Moonen 1* cautiously stated that it was not their intention to assess matters of fact, that is, whether or not the publications were objectionable; they were only to review the administration of the FVPC Act. Instead, the Court merely criticized the Board of Review's lack of consideration of the NZBORA. In spite of this, the Court did make a number of observations. These included that the Board had to be objective and provide reasoning before making a finding.[44] The Court also directed that where a case was "marginal" the right to freedom of expression should trump a finding of objectionability.[45]

The Court of Appeal in *Moonen 2*[46] also refused to revisit whether or not the five step interpretation was adequate, saying it was "complex" and "context dependant". The Court also went further and said:[47]

> Clearly, it [the test] was not intended to be prescriptive. "May" means may. The five-step approach may be helpful. Other approaches are open.

Richardson P reiterated that appellate courts are "restricted to questions of law".[48] This comment immunised the Court, again, from setting out a prescriptive rights-consistent methodology for the FVPC Act. Cheer believes that the lack of development in New Zealand's censorship system is a by-product of the fact that the five-step test is not easy to apply and that although there have been key developments in rights jurisprudence (most notably with the decision of *Hansen*[49]) the OFLC and the Board of Review still appear to follow the *Moonen 1* test.[50] Until similar issues are brought before the courts, where they might identify the discretion creeping into the territory of unjustifiability, it is up to the classification bodies themselves to achieve the right balance. Concerns about this institutional discretion must be faithfully assumed to be mitigated by the fact that this discretion is subject to review mechanisms.

---

[44] *Moonen v Film and Literature Board of Review*, above n 14, at [26].

[45] *Moonen v Film and Literature Board of Review*, above n 14, at [28].

[46] *Moonen v Film and Literature Board of Review* [2002] 2 NZLR 754.

[47] At [15].

[48] At [8].

[49] *Hansen v R*, above n 31.

[50] Cheer, above n 5, at [10.3.2].

III The Internet and the challenges it poses for existing censorship law

This rights context sets a backdrop (albeit an incomplete one) to the first set of questions to be addressed in this thesis: (a) has the Internet created new or just exacerbated already existing problems in the area of censorship; and (b) is the current legal framework set out in the FVPC Act able to address these problems adequately? If the framework is not adequate then the application of the FVPC Act to online expression may lead to poor outcomes for New Zealanders, such as unjustifiable limitations on their rights, and will require reform.

The reason that the Internet is such a problem for censorship law is because of the nexus between the FVPC Act's concern with the availability of expression and the manner in which the Internet stores and delivers information. Further, this technology develops rapidly, meaning multitudinous uses have emerged from the Internet's core function. The novelty brought about by the Internet lies in the interactivity of Internet expression and the multifaceted parties involved in an Internet transaction. The features of the Internet that exacerbate existing problems for law and enforcement include anonymity, the porous global nature of the network and the a-territorial decentralised control of the Internet's infrastructure which facilitates the rapid and ubiquitous spread of information (particularly by foreign speakers) and undermines the certainty of state jurisdiction.

The adequacy of the existing legal framework set out in the FVPC Act is not only undermined by these problems but also by misunderstanding about the Internet and what it enables. Because many aspects of the Internet and online expression do not fit neatly into pre-existing legal concepts, many in the legal community have resorted to using misconstrued analogies to draw conclusions about who should be targeted by the law, why and how. This has fostered broader misunderstanding about the legal status of the Internet. The following section will describe how the Internet works, highlight the problems with law by analogy and then examine the following features of the Internet that create new (and expand existing) problems for law and enforcement:

1. The interactivity of expression;
2. The multiparty nature of Internet transactions;
3. Anonymity;
4. The global network; and
5. The new distribution model.

While this section may generalise to all law and enforcement frameworks, it is also directly relevant to the FVPC Act as a legal framework that applies to online expression. This discussion will also inform the reform recommended in the final part of this thesis.

A How the Internet works

At the outset it is worth briefly describing the technical steps in an Internet transaction in order to put to rest any lingering confusion about what Internet use is. In the most basic terms, when one computer connects to another computer a network is created and information can pass between them. This is made possible by Internet protocol: a rule set by which information is distributed and which requires reciprocity between all participants. The only way the Internet functions as we know it (and why it is so universal) is because of a social compact whereby all users adopt a standard protocol. Using diverse protocols results in diverse "Internets" and to avoid this and to extend the Internet's reach requires a certain degree of homogenisation. One of these protocols is the TCP/IP suite: a system of information developed in the early 1990s and now used by billions worldwide. The TCP (Transmission Control Protocol) aspect is what enables two points to establish a connection and exchange data. The IP (Internet Protocol) aspect specifies how the information is formatted (information is often fragmented into chunks of data called packets) and then how the packets are assigned a host and a location to deliver to (known as addressing). Every time a user connects to a network they are assigned an IP address that can act as an identifier for addressing. This address can be static (a fixed address for a single user) or dynamic (a temporary address for multiple users). Each packet of data carries the IP address of its starting point with it as it travels to its destination. The IP address thus can be associated with a physical location which can identify the user engaging in the particular communication. That said, wireless devices connect via IP gateways rather than hardware, reducing the likelihood of resolving the device to a single identifiable IP address.

The World Wide Web (WWW) is only one of the many systems that operate on top of the suite; others include email, which uses different protocol again. The WWW uses the Hyper Text Transfer Protocol (HTTP): the user requests information from a server and the server returns a response to the user. The WWW is made accessible by web browsers, software applications which allow the user to input the request and then display the response on their device. The response is typically rendered in the form of a web page, that is, documents stored, processed and delivered on at least one server. Given its purpose of information exchange, the Internet is designed to ensure there are as few bottlenecks, or as little congestion as possible, regardless of what the information is, who is using it, where it is being used and whether or not it is legal. There are a number of means of easing congestion including mirroring and caching. Mirroring is a technique where a popular web page is copied and stored on another server, now existing on multiple servers. The user's request is then directed to the server physically closest to them. Caching is where a popular web page is copied and stored on the user device and the user device now acts as a server, removing the need for the external server

to respond to a request for the web page again. The user's device becoming a server in this way reflects the fluidity of the Internet as a network. As it is typically web pages, links and applications that most people deal with (and as this application level engagement has become so normalised and functional) users do not have to be alert to these underlying processes when using the Internet.

It is because of such technicality and jargon that non-technologists analogise the Internet to other communication technologies that pre-existed the Internet (such as post or telephone) in order to reduce the Internet to a simple and workable legal construct. Unfortunately, these analogies do not capture the technical features of the Internet and often end up misrepresenting its capability. Users' relationships with information on the Internet are thus fundamentally different to their relationship with information delivered by other communication technologies. For example, the term "browsing" surfaced to describe the end user's experience of the Internet. However it is not the case that one browses the Internet as one would browse a catalogue or shelf. A user is never exposed to entirely randomised information when they open their web browser. A user consciously makes a request with every click which is logged and stored by default by the server. When a user downloads information, this is copied from the web server or network file server and stored on the device's hard drive, while also still existing on the origin server. When a user opens their browser what they are often confronted with is a carefully curated product based on their historical searches and requests, particularly when the browser is continuously associated with a particular IP address. What the analogy between Internet browsing and browsing a shelf fails to capture is that users are not shown a randomised series of websites to pick from. Instead, Internet users purposefully seek out what is then brought to their device's screen. The FVPC Act, which was not designed with the Internet in mind and has not evolved as quickly as Internet technology, does not clearly or comprehensively set out what Internet expression it applies to, what can be done with that expression and to whom the rules apply. Misconstrued analogy does not help answer these questions.

(i) Interactivity of expression

The interactivity of online expression is a novel issue for censorship law. Online expression subverts traditional legal understandings of expression. For instance, Internet expression is not a fixed construct which maintains its composition as it is sent and received. Internet information exchange is not linear, moving from point A to point B. It is more dynamic and subject to modification along its pathway. Before the Internet, information was also often consumed by individuals in a passive way and their ability to participate in the production of content, alter its presentation, or impact on its further distribution was more constrained.

Sithigh points out that with increased participation, "a greater number of people [are] potential 'producers' or 'creators' rather than mere users or members of an audience".[51] While some aspects of the technology still prevent end users from having complete control over content, this usability is a point of differentiation and marketability. End users are now not mere consumers of information but creators and curators and are more receptive to platforms that allow for this. For example, a majority of Americans who shoot video footage now also post it online and of course these sites typically show high levels of use.[52] End users enjoy yet more participation through comments sections, forums and bulletin boards.

This unfixed, non-linear and dynamic expression is problematic for many areas of the law such as copyright and intellectual property, but it also has implications for censorship. The law seeks to compartmentalise expression in a way that neatly fits into pre-existing legal definitions. In the case of online expression, it is debatable whether the FVPC Act can or should apply to web pages, the video or image that appears on a display, hyperlinks, advertisements, comments or all of the above. Most areas of the law lack sophisticated or nuanced demarcations between online expressive acts and this is certainly true of the FVPC Act.

(ii) Multiparty transactions – more than end users

Another misconception is that the Internet transaction only involves end users and the requests that they make. This is a reductive view, which leads to (for reasons which will be expanded on later in this thesis) disproportionate legal responsibility falling upon end users for expression on the Internet. Internet use is often a series of transactions involving different parties at different points of access. End users are largely only able to behave as they do because of the platforms other parties provide and often only in ways directed, implicitly or explicitly, by these parties. This is elaborated upon by Idisis:[53]

> Although cyberspace may create an illusion that a user has complete freedom and discretion to explore websites and information on the Internet, this is a misconception. In cyberspace, there are only two ways for a user to reach a website: either he knows the exact web address of the website he wants to visit, or he can choose from the links offered by the search engine that he is using. A website that does not fall within one of these two options does not exist for that particular user at that moment. A metaphoric comparison

[51] Daithí Mac Síthigh "The mass age of internet law" (2008) 17 Information & Communications Technology Law 79 at 80.

[52] Mac Síthigh, above n 51, at 80.

[53] Gil'ad Idisis "How to Make Lemonade from Lemons: Achieving Better Free Speech Protection without Altering the Existing Legal Protection for Censorship in Cyberspace" (2013) 36 Campbell L Rev 147 at 159.

> of cyberspace and the real world illustrates the lack of options that a user faces in cyberspace.

This lack of options has implications for the presumption that it is the end user and the end user alone that is responsible for what is brought to their screen and what leaves it.

The ability for those other than end users to control and manipulate expression is in part a product of how Internet transactions are managed (another one of the novel problems brought about by the Internet). At the outset, end users have little control over access to the Internet. This is because end users do not typically connect their devices directly to the Internet. Instead an end user connects their device to a server (a computer which is directly connected to the Internet). Access to these servers is provided by Internet Service Providers (ISPs), which connect to other servers through network access points, thereby increasing the potential extent of the user's connectivity. Smaller ISPs then connect to larger ISPs. The need to go through ISPs is a result of commercial arrangements: ISPs often have exclusivity of access to these servers and end users lack the technical capacity or purchasing power to gain access themselves. The end user inevitably bears some cost for this access. The effect of this is that ISPs become gatekeepers to the Internet and parties to the transaction that ensures that the information reaches the end user who requested it. It is important to add that access is not the only service that ISPs can provide. The industry is becoming more vertical in its provision of services. For instance, ISPs can also host web pages and provide information storage facilities. Amazon (the largest Internet company in the world), for example, is a mobile virtual network operator that provides customers with online shopping and web hosting and has entered the market for entertainment content production and distribution. As a result, defining the legal role of ISPs on the Internet can be challenging and analogy is not particularly useful in this respect. ISPs can be conduits, gatekeepers, custodians, publishers and speakers all at the same time, a role entirely unlike those in the pre-Internet communications industry.

Not only do end users have very little control over access to the Internet but they also have reduced control over what appears on their screens. Other parties have a vested interest in what appears on users' screens because while the Internet is used as a platform to sell goods and services directly to consumers, there is also inherent monetary value in users merely viewing websites and applications (capital sought after by advertisers). Ma points out that this monetisation impacts on the structure and process of the model of content distribution used:[54]

[54] Dan Ma "Push or Pull? A Website's Strategic Choice of Content Delivery Mechanism" (2015) 32 Journal of Management Information Systems 291 at 292.

> Under the conventional pull method, websites are passive. They wait for users to find and visit them by searching, and then initiate the consumption of online content. It is difficult for a website to distinguish itself from competitors who provide the same content and services and adopt similar selling strategies. The pull method waits passively for users to access a website and its content; while the push method allows a website to actively create user demand for new information by periodically informing users of its availability.

The push method is motivated in part by commercial strategies, including targeted advertising. So while Internet companies may be financed more traditionally by investors, these same companies sell their databases of user information to affiliates who will try to convert those users into customers for their products. To this end, search engines use bots to scan all the information on a site which is then analysed and ranked using algorithms designed by the company. The search results then produced by search engines, rendered on the user's display, reflect relevance and rank a site based on the keywords used and whatever underlying motives the search engine has to push information onto the user. Subsequent data mining allows companies to create e-metrics, which provide meaningful information about user browsing. As Levene points out, because search engines are mostly for-profit entities whose obligations are to their paying customers, it is "advertisers" who enjoy the benefit of the search engines' analytics data, not end users.[55] Analytics data allows for "behavioural targeting" where information from user data is used to select which advertisements to display.[56] The user's screen becomes a composite not only of the results of their own requests but of what other parties determine is most profitable to push onto these users. Levene warns that "it is unclear what this [commercial] bias means from the perspective of democratic discourse".[57] And it is also unclear what this commercial bias means from the perspective of user liability. If "choices" are being made for end users by other parties, and if what is presented to them is not solely what they seek out, then end users' autonomous agency and culpability is questionable. It in the least requires re-evaluation of the attribution of legal responsibility to end users alone.

The FVPC Act has few problems dealing with liability in the case of end users and their personal devices. However, if individual New Zealanders are not alone responsible for the availability of objectionable expression in New Zealand, the legal framework must be capable of attributing liability outside the paradigm of the end-to-end Internet transaction, that is, to other parties further upstream.

---

[55] Mark Levene *Introduction to Search Engines and Web Navigation* (2nd ed, John Wiley & Sons Inc, New Jersey, 2010) at 231-232.

[56] Sallaert and Chen "An Economic Analysis of Online Advertising Using Behavioural Targeting" (2014) 38 MIS Quarterly 429 at 430.

[57] Levene, above n 55, at 65.

Ownership (and/or control) of expression is one legal convention that helps attribute liability to a party. However the Internet's infrastructure subverts what would traditionally be understood as ownership and control of Internet technology and thus the expression stored and communicated on this technology. One may think that as New Zealand is a small country, and geographically isolated, that this would narrow the band of potentially culpable upstream parties and make it easier to determine who owns and controls the local infrastructure. As the Internet has physical properties, the starting point for determining ownership and control may well be the hardware: the copper or fibre optic cable, wireless transmission (such as satellite), computing devices, computer servers, modems and routers. Without this hardware there would be no Internet. However, even in New Zealand, this hardware is distributed across a broad range of actors and thus the ownership or control of the Internet is similarly distributed. Decentralised as it is, ownership and control is shaped by contextual factors such as who can finance the expensive infrastructure, as well as conventional market dynamics. The cost of certain necessary Internet hardware is prohibitive for most. For instance, the original construction cost of the Southern Cross fibre optic cable (connecting Australia, New Zealand, Fiji and Hawaii with the United States West Coast) was USD 1.3 billion.[58] New Zealand's telecommunications infrastructure (such as fibre optic cable) is monopolised by a public company, Chorus. Chorus then sells access to this infrastructure to retailers. Physical mobile networks and the thousands of fixed wireless connections are owned by other private parties. Yet the government also has a stake, having invested heavily in public-private partnerships to improve and increase access to this infrastructure. So it is incorrect to suggest that every end user has a proportionate stake in the Internet's ownership model and it is thus difficult to attribute legal responsibility based on this ownership/control paradigm alone. An adequate legal framework would need to account for the ways in which the Internet uniquely subverts such legal conventions.

(iii) Anonymity

Another important feature of the Internet is the potential for anonymity or users' ability to shield their identity. Anonymity is not a novel problem for law and law enforcement but the Internet has normalised anonymity and improved it in sophisticated ways. Anonymity is also regarded as a fundamental benefit of the Internet, as well as a fundamental harm. As Levmore highlights, offensive speakers "find it easy to communicate anonymously and thus to avoid any direct defamation or other legal claims" and this is predictable because "one of the Internet's claims to singularity is the low barrier to entry for provider and user alike, and it is

[58] Southern Cross Cable Network "FAQ" (2012) <www.southerncrosscables.com >.

this very feature that makes juvenile communication so easy".[59] There is a vast range of services designed to meet the demand of end users who wish to be anonymous or pseudonymous online and further to shield their link with a particular physical location, as Larsson and others point out:[60]

> …most common are VPN services or proxies. VPN services in general result in a technically robust anonymity. Common VPN services provide users with the means of avoiding having their IP addresses connected to their offline identity, often in return for a subscription fee. An anonymity service, or anonymity server, is a server that provides the ability to send e-mail, visit web sites, or undertake other activities on the internet anonymously. All traffic between the user (client) and server (host) is encrypted to be indecipherable by third parties.

Additionally, attempts at overcoming anonymity are usually met with new ways of preserving it. While anonymous expression has inherent social utility and that expression would be chilled if anonymity could not be assured, there is no doubt that Internet anonymity shields many offenders from liability for their online behaviour in a manner quite unparalleled in the physical world. Anonymity online is the great challenge to traditional enforcement and problematises theoretical and practical means of localising behaviour to a particular person, determining their location and thus determining which jurisdiction applies to them.

It is this trifecta of interactive and anonymous expression that goes unmoderated, in particular, that causes novel problems for regulators. From a social constructivist perspective this trifecta has been shown to have transformative effects on users themselves. For instance, online expression has been observed as subject to the online disinhibition effect, a psychological phenomenon of "six factors that interact with each other: dissociative anonymity, invisibility, asynchronicity, solipsistic introjection, dissociative imagination, and minimization of authority" which results in expression that does not reflect the "true self" of the individual.[61] Because of this effect, online expressive acts may be more extreme and misrepresentative than their offline equivalents, while at the same time be perceived by the speaker as tolerable or at least shielded from legal consequences. This effect shows that the Internet may have fundamentally altered the contexts where individuals understand their expression as objectionable, illegal or as harmful at all. If individuals 'change' when they are using the

[59] Saul Levmore "The Internet's Anonymity Problem" in *The Offensive Internet: Speech, Privacy and Reputation* (Harvard University Press, 2011) 51 at 57.

[60] Stefan Larsson and others "Law, norms, piracy and online anonymity" (2012) 6 Journal of Research in Interactive Marketing 260 at 263.

[61] John Suler "The Online Disinhibition Effect" (2004) 7 CyberPsychology and Behavior 321 at 325.

Internet (they may, for instance, make a mental switch when they go online), this phenomenon should be accounted for when designing a legal framework that aims to address Internet-enabled harms.

(iv) A global network

These problems (new and exacerbated) are further complicated by the fact that the Internet is not constrained by nationally-drawn borders. Instead, the global climate shapes much of how New Zealanders use the Internet and how New Zealand law might apply to that use. New Zealand-based producers, distributors, intermediaries and other parties are not the only ones responsible for what ends up on the devices of New Zealand users—far from it. Many foreign-based parties' expression ends up circulating through New Zealand networks and it is entirely unclear if and how this is subject to New Zealand law. The global nature of the Internet and the unabridged uptake and implementation of this infrastructure makes regulation problematic for any individual state or centralised body. As Schultz suggests:[62]

> …this was precisely the intent of the creators of the Internet; they connected different, smaller networks together; they taught all those networks to speak a single common language (the Internet Protocol language); they integrated all those lesser networks into a global whole.

Compared to telephony networks of old, Fischer highlights that the Internet is not structured as geographical networks but is based on a global root name system that facilitates sharing, cooperation, and international stakeholder participation.[63] The issue of decentralised control is further explored by Henn:[64]

> One particular entity does not own or control the Internet or the Web. In addition, due to logistical and cultural differences between nations, one regulatory scheme does not exist … Individual national regulation, however, has raised questions about which websites on the Internet such nations have the jurisdiction to regulate.

The subversion of traditional geographical demarcations frustrates states' ability to regulate based on territory alone. Zekos writes that the territoriality principle upon which states rely to

---

[62] Thomas Schultz "Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface" (2008) 19 Eur J Int Law 799 at 803.

[63] Hans Fischer "Technology Perspectives on Code" in Dommering and Lodewijk Asscher (eds) *Coding regulation: essays on the normative role of information technology* (TMC Asser Press, The Hague, 2006) at 45.

[64] Julie L Henn "Targeting Transnational Internet Content Regulation" (2003) 21 BU Int'l LJ 157 at 160.

establish sovereignty and jurisdiction is founded on the "fact of territory".[65] The Internet by contrast is "a-territorial" thus "cyberspace transactions take place concurrently and evenly in all national jurisdictions".[66] A-territoriality undermines legal concepts such as criminal jurisdiction which can only apply to complete or partially complete acts within any one specific territory. Importantly, the FVPC Act derives its authority in part from criminal sanctions.

(v) The Internet distribution market

Change to the distribution market also presents problems for law and enforcement, which has traditionally relied on bottlenecks in the market in order to target resources more effectively. As Tim Wu outlines, where broadcast speech was delivered by a concentrated group of speakers and intermediaries and the telephony market was extremely concentrated and carried speech from "any speaker to any listener", the Internet is an "enormous" number of speakers layered on a few intermediaries resulting in very diffuse speech controlled by intermediaries.[67] In spite of there being fewer intermediaries, Lambers suggests that the Internet now allows a broader division of control and individual autonomy over information production and distribution[68] as shown in the model below:[69]

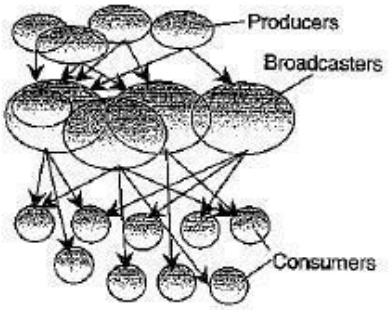


Figure 1 – *Broadcasting*

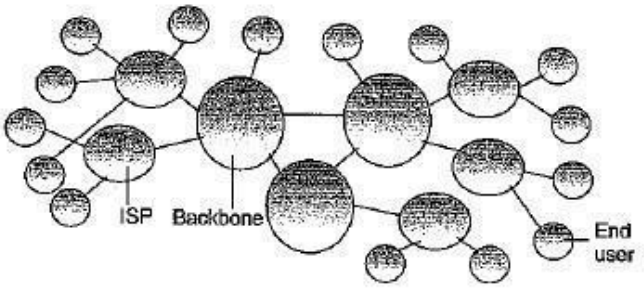


Figure 2 – *Simplified internet model*

This change has not prevented those more concentrated players from the old model attempting to use the Internet to their advantage, arguing for deregulation and the right to control access and distribution of expression absolutely (given in part that they privately own the

[65] Georgios I Zekos "Cyber Versus Conventional Personal Jurisdiction" (2015) 18 Journal of Internet Law 3 at 9.

[66] Zekos, above n 65, at 9.

[67] Tim Wu "Is Filtering Censorship? The Second Free Speech Tradition" in Rossen and Wittes (eds) *Constitution 30: Freedom and Technological Change* (Brookings Institution Press, Washington, 2011) at 94.

[68] Rik Lambers "Speech Control through Network Architecture" in Dommering and Lodewijk Asscher (eds) *Coding regulation: essays on the normative role of information technology* (TMC Asser Press, The Hague, 2006) at 99.

[69] Lambers, above n 68, at 98 and 103.

communication infrastructures).[70] In conjunction with this, the government has consistently facilitated the uptake of the technology as much as possible, only intervening in the market to foster competition where it can between network providers and media organisations. Now telecommunications, media and Internet services are highly concentrated markets in New Zealand. The AUT Centre for Journalism, Media and Democracy has reported that locally, the telecommunications sector continues to consolidate: New Zealand media continue to be increasingly controlled by foreign fund management companies and other unlisted financial institutions (under no mandate to meet public service obligations) and existing companies are competing head to head in online services.[71] This climate has facilitated the process of convergence and highly vertically integrated services whereby New Zealand Internet service providers are involved with the production and distribution of entertainment content. Tambini and others describe this as a "breakdown" of the strict demarcation between different media forms so that there is no obstacle of spectrum scarcity and therefore a non-linear sector has emerged that provides interactive "pull content".[72]

And while New Zealand's telecommunications network still includes traditional delivery hardware such as cable and copper, the market continues to digitise, steadily moving away from such hardware and the importance that ownership of that hardware carries. New Zealand's broadcast services are now delivered by Kordia and TVNZ, state-owned enterprises that are able to transmit to New Zealanders through lease arrangements with American-owned satellites such as the D1 satellite. While these organisations must provide a dividend to the government they are under no public service remit, the TVNZ charter having been abolished in 2011. Thus Internet network ownership mimics other globalised multinational commercial business models. Unsurprisingly, this simultaneous globalisation, local market concentration, convergence and breakdown of demarcations between producers, distributors, intermediaries and other stakeholders has further complicated distinctions between ownership and control and the legal roles and responsibilities that flow from this.

(vi) When these features compound

Internet technology develops in such a way that hastens and intensifies change, overcoming technical barriers and trade-offs with little regard for legal concepts and conventions, and frustrating the adequacy of legal frameworks which rely on settled legal concepts and conventions.

---

[70] Lambers, above n 68, at 99.

[71] Merja Myllylathi *JMAD New Zealand Media Ownership Report 2014* (AUT University, Auckland, 2014) at 1.

[72] Tambini and others *Codifying Cyberspace: Communications self-regulation in the age of Internet convergence* (Routledge, United Kingdom, 2009) at 32.

The generative nature of the Internet meant that it quickly developed well beyond its original protocols. Technologies such as peer-to-peer networking became popular as early as 1999 and "Tor" or onion routing networks became popularised around 2006. Unfettered by regulation, these iterations of Internet technology challenged traditional commercial distribution models and the legal paradigms that underscored them, such as copyright; Elliot describes how "Napster's huge success almost guaranteed some form of retaliation. It came predictably when a number of music companies issued proceedings for copyright infringement."[73] Peer-to-peer file-sharing technology also facilitated the trade of objectionable material, as much as it did pirated music and film. Cloud-computing technology then became popularised in 2008, as did app stores for mobile devices. All of these iterations re-distribute and thus diversify ownership and control interests further. For instance, Reed and Cunningham point out that cloud computing technology offers a "hyper-realised version" of the Internet. Cloud-computing disperses fragmented data in geographically disparate data centres and therefore multiple copies of the data end up in different remote locations (there are dozens of these co-location data centres in New Zealand). Data can exist on numerous servers, in numerous locations, owned by different parties, and that data may only become intelligible with certain protocols and access mechanisms held by certain parties. Producers and distributors of information can now control the scope of distribution of their product, its geographic availability and access more precisely (historically this was limited by the technology where such precise control was trumped by the need for flexible access).[74] This has thrown up the question of whether the producer, the distributor, the owner of the cloud service provider or the owner of the physical server where information is stored should be responsible for the expression therein. Reed has argued that the resource host rarely has control over the information resources hosted on their services and that the controller or end user are those that take steps to make the resources accessible.[75] However, technical backdoors and the ability of parties to remove content from their servers confounds this argument.

This vacillating characteristic, whereby information switches between many servers and devices across the globe, frustrates law and enforcement because as the Internet develops to decrease barriers to information exchange (for instance by increasing anonymity),[76] it decreases barriers for those wanting to exploit the technology for criminal purposes. For

[73] Clive Elliot "The Napster Saga" [2001] NZLJ 291 at 291.

[74] Chris Reed and Cunningham "Ownership and Information in Clouds" in Christopher Millard (ed) *Cloud Computing Law* (Oxford University Press, Oxford, 2013) at 155.

[75] Chris Reed *Internet Law: Text and Materials* (2nd ed, Cambridge University Press, UK, 2005) at 295.

[76] For instance, proxy servers developed to shield IP addresses and are used mainly to this effect.

example, Steve O'Brien, National Manager of the Censorship Compliance Unit at the Department of Internal Affairs) recalls that a Google messaging app "just got absolutely swallowed up by child exploitation offenders to the extent that Google killed it because they were spending too much time responding to law enforcement process servers for the users of that product".[77] O'Brien offers another example where:[78]

> Onion routing represents a heightened level of anonymity/security against third parties analysing and/or intercepting Internet communications, with the added factor…of increased protection against the revelation of the identities of those who send or receive messages, whereas the associated development of the Dark Web provides users with a browsing environment not dissimilar to the Internet, but one that cannot be subject to surveillance.

He describes cloud services, onion routing and child pornography as an "unholy trinity".[79] The line between the harmful expression and the "neutral" technology that enables it can be blurry despite all of the technologists' best intentions. In sum, the Internet has assuredly created new problems and exacerbated existing ones for law and enforcement frameworks. In order to contextualise the subsequent, more focused, discussion about the adequacy of the FVPC Act as a legal framework, it is worth briefly describing the impact of the Internet in New Zealand.

B New Zealand's Internet usage and media consumption

The impact of the Internet is felt sharply in New Zealand as New Zealanders are among the world's most prevalent Internet users. Statistics NZ reports that:[80]

- The number of fiber-based Internet connections has more than doubled to over 100,000 in 2015, from 46,000 in 2014;
- The number of active mobile phone Internet connections increased 7 percent in the year ended June 2015, to 3,959,000; and
- The number of broadband Internet connections with no data cap has quadrupled to 628,000 in 2015, from 155,000 in 2014.

The uptake has also been striking. In 2012, Statistics NZ reported that 1.3 million New Zealand homes (80 percent) had some form of Internet connection. Laptops, tablets, and smartphones

[77] Interview with Steve O'Brien, Censorship Compliance National Manager (the author, Wellington, July 2015).

[78] Mark O'Brien "The Internet, child pornography and cloud computing: the dark side of the web" (2014) 23 Information & Communications Technology Law 238 at 245.

[79] O'Brien, above n 78, at 247.

[80] Statistics NZ "Household Use of Information and Communication Technology" <www.stats.govt.nz >.

are now the most popular means for New Zealand users to connect to the Internet. As of 2014, there are reportedly 1.98 million subscriptions to ISP broadband services and 3.7 million Internet-connected mobile devices circulating in New Zealand.[81] The World Internet Project New Zealand reported that most people report that they use the Internet to surf or browse the web (96%), check their email (89%) or visit social networking sites (81%); almost two-thirds download free mobile applications ("apps") (65%), and over a third use cloud technology (34%) and purchase apps (41%).[82] The vast majority of those who use social networking sites post messages (82%) and post pictures, photos or videos (71%).[83] Further, over two thirds of Internet users at least occasionally watch TV shows online (70%), and a significant number listen to radio stations through their Internet connection (45%), download or stream feature films (38%) and download or stream music and video on a daily basis (20%). Half of Internet users play games online at least occasionally. More than a quarter of respondents said that they look at sites with sexual content at least occasionally.[84]

Despite this high and varied use of the Internet and its applications, repeat screenings and reality-TV dominate local television content and profit imperatives continue to drive the sourcing of commercial, advertising friendly content.[85] The NZ Media Ownership report has a foreboding conclusion: that because of changes in the media landscape, New Zealand's public sphere is shrinking.[86] Therefore the increase in use of a technology that enables expression does not correspond with an increase in public interest media. While theoretically democratic, it is questionable whether global connectivity and exponential information exchange realises the free expression justifications of truth-seeking and democracy if measured by increased civic engagement.

In terms of the broader content production and distribution climate, international print media is in a state of "turmoil" and multibillion dollar ownership deals continue to recalibrate the entertainment, media and technology sector.[87] Additionally, claims that the Internet would displace traditional media are said to be exaggerated.[88] Although there are now many new

[81] Statistics NZ "Internet Service Provider Survey: 2014" <www.stats.govt.nz >.

[82] The World Internet Project New Zealand *The Internet In New Zealand 2013* (AUT University Institute of Culture, Discourse and Communication 2013) at 12.

[83] The World Internet Project New Zealand, above n 82, at 12.

[84] The World Internet Project New Zealand, above n 83 at 10.

[85] Myllylathi, above n 71, at 48.

[86] Myllylathi, above n 71, at 50.

[87] Myllylathi, above n 71, at 2.

[88] See generally An Nguyen and Mark Western "The complementary relationship between the Internet and traditional mass media: the case of online news and information" (2006) 11(3) Information Research 151.

sources of information on the Internet, the rise of this technology has not coincided with a rise in a centralised or collectivised distribution of information which would undermine the traditional media model. Instead, as with traditional media, online communication and expression has been commodified. Indeed, traditional media has evolved to some extent, with owners re-conceptualising their products and services into online equivalents. That the Internet has been commercialised and made profitable reflects rather than subverts traditional mass media.

Highly concentrated, vertically integrated markets coupled with foreign ownership undoubtedly impact on the state's ability to intervene in the production and distribution of content. This directly affects New Zealanders who consume large quantities of foreign entertainment content. Therefore, the Internet, the future of this technology and any regulation of it, is, and will be a significant part of New Zealanders' everyday experience.

Having determined that the Internet has created novel, and exacerbated existing, problems in the area of censorship law, the next question to address is whether the existing legal framework set out in the FVPC Act is able to address these problems. The foremost challenge for the FVPC Act is to target the behaviour it seeks to regulate, out of the huge breadth of expression that the Internet permits (both coming into and out of New Zealand), without undermining the features of the Internet that make it so popular or unjustifiably infringing on the right to freedom of expression. The law did not develop synchronously with the arrival of the Internet or as Internet use expanded. Questions hang over whether the FVPC Act applies to whatever a New Zealand user requests to be rendered on their device. There is no settled view as to what constitutes a publication with respect to the Internet, nor what may be done with it, nor to whom the FVPC Act applies. There is also a disconnect between what people believe is legal, the law and how the law is applied to their expression. Rowbottom warns, for instance, that:[89]

> Now that those comments can be made available to the world at large and remain recorded and searchable, such expression has greater potential to come to the attention of prosecutors and litigators. The result is that people enjoy greater freedom of expression, in that they can communicate with a wider range of people in different places and times than before, yet people's everyday expressive activities are potentially subject to more regulation.

[89] Jacob Rowbottom "To Rant, Vent and Converse: Protecting Low Level Digital Speech" (2012) 71 Cambridge Law Journal 355 at 356.

Additionally, as users store content less and less on personal devices but instead on external servers, potentially in other jurisdictions, liability and jurisdiction become less certain. It will be argued that the current legal framework has not been able to manage and meet the challenges described head on, indicating that it may not be adequate as it is. Obvious gaps in the FVPC Act and poor interpretation of the law (at times) have contributed to this inadequacy, and are discussed further below. If it is to apply to online expression and as one of the only means of Internet regulation, the FVPC Act should be robust and fit for that purpose.

C Dispelling the myth of a libertarian tradition of censorship – international public and private case studies

It is necessary to address the illusion that the Internet is not regulated or subject to censorship. While the Internet creates new problems and exacerbates existing ones for legal frameworks, ideological myths and inaccuracies too burden the adequacy of legal frameworks as they apply to the Internet. This particular illusion sustains an ideological myth that the state cannot or should not regulate the Internet. The climate is one of much technological, economic, social and political change and one which confounds and challenges existing legal frameworks. Yet, many states have not shied away from the challenges which the Internet poses and do not subscribe to this view, particularly Western liberal democracies. State censorship is a common practice globally. The case studies set out below will demonstrate this. Therefore the idea that the Internet is an open unmoderated space (free from censorship) is entirely theoretical. As a result, the censorship of expression on the Internet in New Zealand is not an anomaly when compared to the practice of other comparable states. In fact, New Zealand's strategy is relatively inert and less developed than other comparable states. This section sets out the many ways in which the Internet is in fact censored by states or by Internet companies that provide services and platforms. This section should dispel any lingering suggestion that the Internet is not censored or that New Zealand should resist engaging in censorship because it would be out of step with liberal and/or progressive state approaches to Internet regulation.

(i) State censorship

The best example to start with may well be New Zealand's closest geo-political neighbour. Rather than having disparate uncoordinated regulatory agencies for different types of expression, Australia has a centralised communications regulator: the Australia Media and Communications Authority (ACMA), which oversees all regulation of expression. Regarding the Internet specifically, online content is investigated and actioned under the laws found in Schedules 5 and 7 of the Broadcasting Services Act 1992 (Cth) by the ACMA (collectively known as the Online Content Scheme). The ACMA works with the Classification Board to have online material classified and then makes determinations as to whether such material can

be hosted in Australia. The ACMA is empowered to order the take down of Internet material so that it cannot be accessed from Australian servers. This has earned Australia the reputation of being one of the strictest censorship regimes in the West.[90]

While the United Kingdom takes a tiered approach to the regulation of expression, it has kept abreast of the changing marketplace. Entertainment is dealt with by the communications regulator Ofcom (broadcasting), and the British Board of Film Classification (BBFC) (non-broadcast material). The BBFC has been more involved in government regulation through the Video Recordings Act 2010 and the Digital Economy Act 2010. The BBFC has been designated by the government as the body for classifying video games, music videos, and mobile phone content, providing certifications for this material, and thereby this private organization is responsible for much censorship activity in the UK. Similarly, the Internet Watch Foundation (IWF), an independent registered charity, operates in informal partnership with government to identify obscene material online. This approach has not escaped criticism. Laidlaw argues that the IWF was a product of direct government threats and thus it carries out a function that is essentially governmental in nature.[91] The set-up is less clearly self-regulatory and, as a public authority, is arguably operating without any legal basis, consistently failing to show evidence that its operation is not arbitrary.[92]

In 2007, the Home Office demanded that all UK ISPs sign up to the blacklist created by the IWF or the government would be forced to legislate. The majority complied and, as Edwards points out, the government was able to put in place a universal non-transparent scheme of online censorship without public debate, new laws or a system of public accountability.[93] The government's appropriation of these private organizations allows state censorship to occur while avoiding public transparency and accountability mechanisms. (Currently) as a member of the European Union, the UK is also subject to the range of Conventions, Directives and Framework Decisions created to address cybercrime, including criminal expression. One product of harmonisation has been significant developments in civil case law concerning ISP liability. UK courts are now deciding that those UK laws which implement EC directives require that innocent ISPs (who are "essential actors in all of the communications"), not only

[90] Deibert and others "Australia and New Zealand" in *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace* (MIT Press, Cambridge (Mass), 2010) at 391.

[91] Emily B Laidlaw "The responsibilities of free speech regulators: an analysis of the Internet Watch Foundation" (2012) 20 International Journal of Law and Information Technology 312 at 325.

[92] Laidlaw, above n 91, at 329.

[93] Lilian Edwards "Content Filtering and the New Censorship" (paper presented to IEEE, February 2010) 317 at 318.

need to make access to illegal material more difficult but that they must bear the cost of introducing those measures.[94] The EU is mainly concerned with "creating regulation which promotes the proper functioning of internal markets" so it follows that "the genesis of EU competence in criminal law is therefore not one based on the rationale of harmonization but rather on cooperation"; the EU's transition into criminal law (and online criminal law specifically) is thus likely to be a more overt expression of political identity.[95] The UK example (subject as it is, for the moment, to the EU developments) shows that there are ways for a state to both retain national law-making identity alongside increasing efforts at multinational legal harmonisation with respect to the challenges created by the new globalised distribution of expression.

Even in the United States, where censorship would seem to be the antithesis of the First Amendment of the United States Constitution, expression is regularly censored either by the government or by private parties. For instance, the Motion Picture Association of America assigns films ratings which are overseen by the Classification and Rating Administration. These ratings are not legal or enforceable but the majority of films carry the ratings (online and offline) and the vast majority of American cinemas only exhibit rated films, thereby voluntarily submitting to the rating system. Because of the extent of the exhibitors opt-in, these agencies enjoy a high degree of control over the content of films and thus the public is still subject to widespread and standardised censorship. The Federal Communications Commission deals with all other types of content, from the regulation of broadcasting through to the regulation of ISPs. Some states' attempts to regulate material on the basis of it being specifically harmful to minors have been challenged on First Amendment grounds[96] but there is a range of federal and state obscenity laws which are enforced by a number of agencies.[97] Further, over half of the world's top 20 .com companies are domiciled in the United States and readily declare they are only subject to the jurisdiction of the United States, despite having regional offices and headquarters in other countries. Given the global reach of these powerful entities, Internet regulation is disproportionately affected by United States' censorship

[94] See for instance, the recent case of *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors* [2016] EWCA Civ 658 at [143]: "These immunities from infringement and any requirement to monitor plainly support and benefit the businesses of intermediaries such as the ISPs. Moreover, as the judge himself said in *20C Fox v BT (No 2)*, the intermediaries make profits from the services which the operators of the target websites use to infringe the intellectual property rights of the right holders, and the costs of implementing the order can therefore be regarded as a cost of carrying on the business".

[95] Erik O Wennerstrom and Csaba Sandberg "Combating Cybercrime - Developments in the European Union" (2010) 56 Scandinavian Stud L 247 at 272 and 283.

[96] *Brown v Entertainment Merchants Association* 564 US 08-1448 (2011).

[97] Obscenity 18 USC § 1460-1470.

precedent or lack thereof. For example, while censorious in respect of media content, blanket immunities were given to US online service providers for the third party content hosted on their services by virtue of s 230 of the Communications Decency Act 1996. This was interpreted by the Fourth Circuit Court of Appeal in the case of *Zeran v American Online Inc* to mean that online service providers were immune even in the case where they have knowledge of the actionable (in this case defamatory) content.[98] Materna notes that subsequent affirmation of the *Zeran* standard has meant that "s 230 jurisprudence took a dangerous step toward allowing ISPs carte blanche to host any content they wish with virtually no liability".[99] The presumption has been ISP immunity since. The position in the United States has made it difficult for other states who wish to regulate online service providers (who defer to this precedent). Furthermore, ISPs (particularly social media service providers) often require that a person be over the age of 13 years to use their services. Rather than flowing from corporate social responsibility, this is to ensure compliance with the Children's Online Privacy Protection Act 1998, a piece of United States Federal legislation which places a range of obligations on online service providers regarding the collection of personal data and privacy of young persons. In these and other ways, the United States has become a great exporter of legal standards for online activity challenging the ability of other states to carve out a unique regulatory position.

Even though this is by no means a comprehensive comparative review, the existence of a state classification system in New Zealand is not out of step with international examples. However New Zealand's regulatory strategy is less developed and even inert compared to the strategies adopted by other comparable countries. Regardless of whether New Zealand is more or less censorious than other comparable countries, it certainly lacks identity and strategy with respect to Internet regulation.

The differences in approaches taken by different states indicate that even in an era of globalization and intervention, states still take an isolationist approach to the practice of censorship. More, rather than less, state censorship is likely. Deibert and Rohozinski suggest that this ubiquitous state censorship is due to the fact that "states no longer feel the pariah status by openly declaring their intent to regulate and control cyberspace. The convenient rubric of terrorism, child pornography, and cyber security has contributed to a growing expectation that states should enforce order in cyberspace, including policing unwanted

[98] *Zeran v America Online Inc* 129 F 3d 327 (4th Cir 1997).

[99] Mark G Materna "Protecting Generation Z: A Brief Policy Argument Advocating Vicarious Liability for Internet Service Providers" (2012) 47 USF L Rev 109 at 117.

content … Internet censorship is becoming a global norm."[100] While censorship has been stigmatised as misaligned with democratic values (particularly by libertarians), it is now accepted as a necessary part of a well-functioning democracy (as has always been the case in New Zealand).

That said, the organisation of the Internet means that targeting individual speakers is costly and futile thus finding alternative targets of enforcement and/or cooperating with the owners of private infrastructure is increasingly necessary. Jewkes notes that, in a context of change and the emergence of new social coordination and governance (an offshoot of neoliberalism), the state is eschewing top-down delivery of social order by externalising responsibility onto extra-governmental actors.[101] Balkin's believes this "new-school speech regulation" is a way to legitimise state conduct without overt and excessive displays of power:[102]

> It is far better to control digital networks in the background or behind the scenes, so that control and surveillance seem indistinguishable from normal conditions rather than singular or intermittent displays of extraordinary force. To achieve these goals, states can either own Internet intermediaries or exert control over privately held intermediaries. The latter strategy leads directly to practices of collateral censorship.

Balkin predicts that this strategy where governments "co-opt private infrastructure to do the government's work" will mean that "[i]n the digital age, this may be the major function of prior restraint".[103] For example, the IWF (not the UK government) creates blacklists of websites which ISPs block access to. And of no small consequence, while this extra-governmental censorship relieves the public cost of law enforcement, it places responsibility for crime prevention largely upon potential victims who must protect themselves by purchasing security goods and services.[104] If users want to avoid objectionable expression, they must purchase filters and use other available mechanisms while still risking coming into contact with it. Some of these consequences echo across New Zealand's regulatory strategy and it will be later argued that this erodes the purposes of the FVPC Act and the right to freedom of expression.

(ii) Private censorship

---

[100] Deibert and Rohozinski "Beyond Denial" in Deibert (ed) *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace* (MIT Press, United States, 2010) at 4–5.

[101] Yvonne Jewkes "The Private Policing of Internet Crime" in Jewkes and Yau (eds) *Handbook of Internet Crime* (Routledge, Oxford, 2011) at 553.

[102] Jack M Balkin "Old-School/New-School Speech Regulation" (2013) 127 Harv L Rev 2296 at 2309.

[103] Balkin, above n 102, at 2338.

[104] Jewkes, above n 101, at 553.

To advocate that the Internet should be free from censorship is also to ignore the fact that there are plenty of examples of private entities such as Internet service providers censoring the Internet in various ways. It can take on many different forms, such as cooperation with states to apply filters or take down content or merely setting out standards of use in their terms of service and cutting off access to their services by those who breach those terms.

Search engines have cooperated with many countries to meet particular regulatory requirements. Yahoo! launched a Chinese search engine in 1999 and Google followed suit in 2006. Both sites informally comply with Chinese filtering laws and are thus complicit in China's censorship strategy.[105] In Germany, "Google has agreed to self-censorship of sites, which are indicated on the list of the Federal Agency for Media Endangering Youth".[106] Both examples reflect the unique cultural context of the states involved but what is similar is the dependence on private cooperation to be effective. Marsden observes that this type of private censorship has been increasing over the last decade despite sweeping "three wise monkeys" immunities protecting these companies from liability for third party content.[107] The situation created a paradox where these private entities enjoy immunities from liability for criminal activity that takes place on their platforms (thanks to the US precedent) while actively monitoring and censoring expression. This is more problematic because whether they are complying with state law or applying their own standards, they censor with potentially unscrupulous authority. For example, following YouTube's censorship of a Syrian channel at Senator Joe Lieberman's request, Rosen noted that "a user-generated system for enforcing community standards will never protect speech as scrupulously as unelected judges enforcing strict rules".[108]

Individuals are also subject to yet more tacit censorship by the very structure and arrangement of these services and platforms. Yu identifies that YouTube, Apple iTunes and even cloud providers have begun to impose geographical restrictions, create regionally based walled

---

[105] Jessica E Bauml "It's a Mad, Mad Internet: Globalization and the Challenges Presented by Internet Censorship" (2010) 63 Fed Comm LJ 697 at 701.

[106] Yulia A Timofeeva "Censorship in cyberspace: new regulatory strategies in the digital age on the example of freedom of expression" (Doctoral Thesis, Universität, 2005) at 66.

[107] Christopher Marsden "Network Neutrality and Internet Service Provider Liability Regulation: Are the Wise Monkeys of Cyberspace Becoming Stupid?" (2011) 2 Global Policy 53 at 54.

[108] Jeffrey Rosen "The Deciders: Facebook, Google and the Future of Privacy and Free Speech" in Rosen and Wittes (eds) *Constitution 3.0: Freedom and Technological Change* (Brookings Institution Press, Washington, 2011) 69 at 81.

gardens and largely undermine declarations as to the globally accessible nature of content.[109] Yu predicts that an outcome of this is that users may shift to illegal sites that distribute content without restriction.[110]

Private actors also engage in censorship by mob or "hit" popularity. Mellor supports this proposition with the following example, "A putative speaker can set up her own website but the likelihood is that it will receive substantially less traffic than established ones".[111] The search engines that enable preferential access to such established sites are not designed to seek out truth, in fact they, as Mellor says, make it "harder to come by". In effect, popular expression is promoted, viewed by many, and unpopular expression is demoted to the dark unseen spaces of the Internet. Such is the fear of Cass Sunstein who argues that a distribution of speech rights determined by a market pricing system would foreclose disfavoured or unpopular speech.[112] Both geographical restrictions and hit popularity are simple but effective means of censorship, particularly given their subtly. Users will be less cognisant of the encroachment and are less likely to notice these subtle shifts in their Internet experience.

The spectrum and practice of this private censorship activity is largely unknowable, as suggested by Idisis:[113]

> It is unknown whether there is a set of rules that apply in these [content blocking/take down] decisions, the thought process that the decision is based on, and how much weight, if any, is given to the advancement of free speech. A look at the terms of service of different service providers is even more troubling and does not shed any light on these questions.

Others, including Heins, suggest that judicial determinations of content must be "just the best guess of Facebook censors".[114] Participation in the discourse that determines what is censored is only available to a few. An individual may decide not to use online services, but this would be to decide to not participate in an increasingly universal human activity. It is also not viable to do away with these monolithic and monopolistic entities because, as Thompson suggests,

---

[109] Peter Yu "Towards the Seamless Global Distribution of Cloud Content" in Cheung and Weber (eds) *Privacy and Legal Issues in Cloud Computing* (Edward Elgar Publishing, United Kingdom, 2015) at 187.

[110] Yu, above n 109, at 191.

[111] Samuel T Mellor "Regulating Online Conduct: Conundrums and Spatial Metaphors in the Wild West" (LLB (Hons) Dissertation, University of Otago, 2011) at 35.

[112] Cass Sunstein *Democracy and the Problem of Free Speech* (The Free Press, United States, 1993) at 57-58.

[113] Idisis, above n 53, at 155.

[114] Marjorie Heins "The Brave New World of Social Media Censorship" (2013) 127 Harv L Rev F 325 at 326.

"some online intermediaries may indeed be so integral to the public marketplace of ideas that when they deny service, this produces a speech deficit that cannot be wholly alleviated through alternative pathways for speech."[115] While these entities may be receptive to human rights and freedoms and engage in socially responsible ways, there are few sources of power able to resist and otherwise challenge their censorship clout. The decision to censor is determined the by hierarchy of power, with corporate interests situated at the top. For example Google boasts, "WE always assess the legitimacy and completeness of a government request [to remove content]".[116] Governments must in turn carefully negotiate their relationships with these entities so as not to alienate the benefits of access to the infrastructure and services which are privately owned and monopolised.

New Zealand now finds itself at a cross-road: address the ways in which the Internet has undermined the adequacy of our current legal framework or cede legal authority to other jurisdictions or the private entities that have monopolised the Internet (particularly given that they are assiduously censoring the Internet New Zealanders use irrespective of New Zealand's censorship strategy). If the former road is adopted and if it is to withstand future challenges posed by new and disruptive technology, the FVPC Act will require reform.

IV The Films Videos and Publications Classification Act—the current state of the law, weaknesses and inadequacies

This section will focus on a sample of aspects of the legislation that have been challenged by the disruptive nature of Internet technology. This is by no means a comprehensive account of all the weaknesses and inadequacies of the FVPC Act, but a starting point. This account will describe the state of the law and why some reform is necessary. Before turning to the specific aspects of the FVPC Act, this section first addresses two important preliminary matters. First, it outlines two Internet regulation theories. These theories have shaped thinking and decision-making about law on the Internet and shed light on why the law has developed in the way that it has. Secondly, it provides an account of the recent legal history of the statute. This history also deals with the rise of and proliferation of the Internet and furthers the previous discussion about the cultural impact of the Internet in New Zealand. Both parts contextualise the subsequent substantive discussion which focusses on the following aspects of the FVPC Act:

---

[115] Stephen James Thompson "Protecting Legitimate Speech Online: Does the Net work?" (LLB (Hons) Dissertation, University of Otago, 2012) at 14.

[116] Google "Google Transparency Report" (2015) <www.google.com/transparencyreport/ >.

a) the statute's mechanism for capturing expression, that is, the difficulty with interpreting the term "publication";
b) the now superfluous types of offences under the FVPC Act and the poor interpretation of these offences by the courts;
c) the difficulty with attributing liability to foreign parties who make available objectionable expression in New Zealand;
d) the magnification of jurisdictional uncertainty; and
e) the restricted enforcement approach adopted in New Zealand as a result of the foregoing issues.

In aggregate these discrete issues represent a wider, more systemic disconnect between the law's purpose and its ability to achieve that purpose.

A Theoretical influences on censorship laws and judgments

Before proceeding to the specific aspects of the legislation that have been challenged by the disruptive nature of Internet technology, it is worth briefly mentioning two theories that help characterise the law's relationship with the Internet. Even if not referred to explicitly, the principles of these theories underlie the decision-making of lawmakers and the judiciary. As a result, understanding these theories is one way of providing context to the development of the law and the condition it is now in. The first theory is *functional equivalence* or the belief that the law should treat similar activity the same, regardless of whether the activity occurs online or offline. The other is *internal versus external perspectives theory* which asks whether the law is regulating the individual and their behaviour or merely the physical technology that enables it. The case law discussed below will show the role that these theories have played in the law's development.

Functional equivalence is a theory which presumes that law that existed prior to the Internet is capable of being applied to activity enabled by the Internet. A law that achieves this is considered "technologically neutral". Reed suggests that functional equivalence can be either the direct application of an existing law to online activities or its use as a guiding principle (i.e. that the existing law should guide how equivalent online activity should be treated).[117] Reed and Brownsword both highlight that if the law is radically different for online and offline activity, individuals are forced to make mental switches once they go online because of the

[117] Chris Reed "Online and Offline Equivalence: Aspirations and Achievement" (2010) 18 Int'l JL & Info Tech 248 at 251.

lack of analogy.[118] However, Reed also cautions that there is a "temptation" to seize upon the similarities between online activity and existing offline activity and ignore the differences.[119] Thus where the activity is not actually equivalent, a new "rule-set" or law needs to be made. Zekos is also sceptical about the utility of functional equivalence as "no one metaphor, or legal parallel, will reflect the myriad nature of this internet".[120] In the context of defamation, Judge David Harvey highlights that functional equivalence can be problematic for this "paradigmatically different form of information communication".[121] Further, in some contexts (such as copyright law) functional equivalence has been "impossible to achieve".[122]

Functional equivalence has been a guiding principle in New Zealand law to a certain extent. For instance, both the Electronic Transactions Act 2002 and the Copyright Act 1994 contain provisions for the equal treatment of both electronic and offline activity. Functional equivalence has also been a guiding principle in case law.[123] The case of *Murray v Wishart* is emblematic of functional equivalence in action. The Court of Appeal drew on analogies between the online activity of posting comments on a Facebook page and offline activities such as news agents,[124] graffiti on walls[125] and public meetings[126] before determining that a golf club wall was the "most appropriate analogy" to the online activity in question.[127] This indicates that, despite criticisms, functional equivalence has weight in New Zealand law as a guiding principle.

As to internal versus external perspective theory, this is based on the idea that conduct on the Internet can be legally understood from two contrasting perspectives. Orin Kerr summarises these as follows:[128]

---

[118] Roger Brownsword "The shaping of our on-line worlds: getting the regulatory environment right" (2012) 20 International Journal of Law and Information Technology 249 at 252.

[119] Reed, above n 117 at 265.

[120] Georgios I Zekos "State cyberspace jurisdiction and personal cyberspace jurisdiction" (2007) 15 International Journal of Law and Information Technology 1 at 36.

[121] Judge David Harvey "Recent Developments in On-Line Defamation" (paper presented to NZLS CLE IT & Online Law Conference, May 2015) at 164.

[122] Judge David Harvey *internet.law.nz* (3rd ed, LexisNexis NZ, 2011) at [10.9].

[123] See Heath J's comments in *R v Hayes* (2006) 23 CRNZ 547 (HC) at [45] and [46]. This was later applied in *R v D* [2011] NZCA 69 at [64].

[124] *Murray v Wishart* [2014] NZCA 461, [2014] 3 NZLR 722 at [128].

[125] At [131].

[126] At [132].

[127] At [143].

[128] Orin S Kerr "The problem of perspective in Internet law" (2003) 91 Georgetown Law Journal 357 at 359-360.

> … the internal perspective adopts the point of view of the user who is logged onto the Internet and chooses to accept the virtual world of cyberspace as a legitimate construct … The external perspective adopts the viewpoint of an outsider concerned with the functioning of the network in the physical world rather than the perceptions of the user.

Kerr suggests that, when applying the law, either perspective can be adopted with very different results:[129]

> [To the internal observer] we look for analogies between cyberspace and "realspace" and try to match rules between them. To the external observer, in contrast, the Internet is a physical network and we apply law to the Internet by applying the law to the electronic transactions underlying the network's operation.

The problem is that neither perspective has greater legitimacy than the other. However, every time the law is applied to the Internet only one perspective can be adopted and this perspective must be adopted consistently.[130] This consistency is necessary for legal certainty and ensures that parties are not allowed to avoid the law by shifting between the two perspectives.[131]

It is Kerr's preference that when the user subjectively understands that their conduct as "offline" an external perspective should be adopted, and conversely when the user subjectively understands their conduct as "online" an internal perspective should be adopted.[132] Yulia Timofeeva sensibly identifies the parallels between the perspectives theory and the more well-known space versus network theory: the Internet conceptualized as a public space versus a private network of connections.[133] Timofeeva suggests that legislators need to clarify which perspective is intended when statutes are drafted before inconsistencies overwhelm the law.[134] Murray also emphasises the potential for harm when individuals do not appreciate the effects of their online activity on the real world.[135] Inconsistency across laws and within areas of the law exacerbates this.

---

[129] Kerr, above n 128, at 361.

[130] Kerr, above n 128, at 357.

[131] Kerr, above n 128, at 405.

[132] Kerr, above n 128, at 396.

[133] Timofeeva, above n 106, at 36.

[134] Timofeeva, above n 106, at 41.

[135] Andrew Murray *Of Cyberspace: Control in the Online Environment* (Routledge-Cavendish, United Kingdom, 2007) at 210.

There is little evidence of overt consideration of the perspectives theory or space versus network theories in New Zealand law. The extensive discussion as to whether data constitutes property in *Dixon v R*[136] exemplifies the dangers of not adopting a perspective when drafting law and how this lack of perspective can cause individuals to misunderstand the law, later requiring clarification by the courts or revision by Parliament. There is evidently a need for greater reflection on perspectives theory by New Zealand lawmakers.

The next section will address the recent history of the FVPC Act and identify in part why a more principled approach has not been taken by New Zealand lawmakers to the FVPC Act. Generally speaking lawmakers have never given due weight to the impact the Internet has had on expression and the ability of regulators to censor expression. Instead, the statute has been layered with cosmetic amendments that do not holistically address compliance and enforcement challenges. As will be seen, these shallow amendments have ignored the perspectives and space versus network theories and/or frustrated the ability to interpret the law with these theoretical perspectives in mind.

B A short history—from enactment to today

Due to the complex nature of censorship, there have been and perhaps always will be interpretative issues with censorship legislation. Responsibility for these interpretative issues falls largely on the shoulders of the technological changes of the 20th and 21st centuries. Every time a new expression-facilitating technology has appeared (as was the case with film, television, VCR, DVD and the Internet), the New Zealand government has championed the uptake of the technology. Subsequent attempts at censorship of these technologies is reactive and cosmetic, and rarely future-proof or capable of enduring without frequent amendment.

The FVPC Act did not appear out of a regulatory vacuum in 1993. In fact it was only the latest iteration of a long-standing tradition of state censorship in New Zealand, dating back to British colonisation. The enactment of the FVPC Act was specifically a response to its contemporary context. Its main purpose was to consolidate pre-existing separate censorship regimes (with the exception of broadcasting), aspiring to meet the challenges which the then new technology (such as video cassette) posed. The Minister of Social Welfare of the day, Jenny Shipley, said that the censorship regimes were "untidy" and allowed for "manipulation".[137] Borrowing heavily from past statutes, and enshrining long-standing censorship principles, the FVPC Act also reflected a relatively recent ideology of state paternalism. It was the state's responsibility

[136] *Dixon v R* [2015] NZSC 147.

[137] (2 December 1992) 532 NZPD 12758.

to prevent harm rather than individuals or industry. On the interaction of harm, personal freedoms and the government's responsibility, Shipley said:[138]

> Some will argue that that is a matter of personal rights or freedom. That is not my view, nor is it the view of many thinking New Zealanders, for it is women and children who are almost always the victims of such indulgence. The Government has decided to introduce the Bill taking that firm stand … In future it will be the responsibility of individuals to face up to this issue, rather than the wider society always being left to prove damage as has been the case in the past.

Although aspirational, the lack of foresight on the part of the statute's architects is exemplified by the fact that Parliament was urged to address the issue of new technologies such as "video-phones", "computer bulletin boards", "Sky television" and "live sex videos" in the statute.[139] However, such recommendations were not included in the final draft of the Bill and this would not be reviewed for a number of years.

(i) Technological change

While the FVPC Act did not pre-date the Internet, its architects did not anticipate the many ways in which this technology would subvert the statute's purpose. The technological change that followed the introduction of the Internet very much changed the landscape in which the statute operated, and quickly. Academics and corporations had been experimenting with and trialling computer connectivity technology in New Zealand since the late 1980s.[140] Internet applications such as Bulletin Board Systems and Internet Relay Chat quickly followed. The PacRim undersea fibre optic cable construction was completed in 1995 and the Southern Cross Network Cable began construction in 1998.[141] These cables would "connect" New Zealand's telecommunications infrastructure to the rest of the world. By the end of 1995, it was estimated that 100,000 New Zealanders were online, commercial operators had outstripped academic operators and Internet cafes had emerged.[142]

Very soon after the statute's enactment new technologies were introduced to the New Zealand market. For example, in 1995, DVDs (Digital Virtual Discs) were created and quickly adopted

---

[138] (2 December 1992) 532 NZPD 12761.

[139] (2 December 1992) 532 NZPD 12767.

[140] Down To The Wire "1989: It Came Without A Manual" (22 July 2015) < http://downtothewire.co.nz/the-beginning-1989/>.

[141] Southern Cross Cable Network "Overview and Map" (22 July 2015)
< www.southerncrosscables.com >.

[142] Down To The Wire, above n 140

by entertainment distributors as the preferred distribution format of media content. Wanting to facilitate the uptake of this technology in New Zealand, Parliament amended the Copyright Act 1994, removing the prohibition on parallel importing in order to drive down the cost of the technology.[143] It predictably became a household staple. Not specified as an example of a publication, DVDs did not fit neatly into the s 2 FVPC Act categories of publication. However, the OFLC acknowledged the importance of "keeping abreast" of new technology[144] and it was determined that DVDs did indeed meet the definition of a publication without much furore. The Chief Censor of the day identified that the emergence of such technologies were producing "interpretative challenges".[145] It is worth noting that the interpretation problems and other challenges the Internet has presented look even more extreme compared to the relative seamlessness of this transition to DVD technology.

Concerned with the potential harmful impact that Internet technology could have in New Zealand, Trevor Rogers MP introduced the Technology and Crimes Reform Bill 1995. The Bill hoped to create new offences for the misuse of telephone lines to transmit objectionable material and prohibit communication with foreign telecommunication services hosting "objectionable" images. The Bill would also require ISPs to cut off links to foreign websites on the order of the Office of Film and Literature Classification. It is worth noting the foresight of the Bill, in light of the measures that states are taking to censor expression on the Internet nowadays. At the time, however, the Bill was considered unworkable and unnecessary, and was later defeated in Parliament.[146] This was not followed up by an inquiry or an alternative regulatory strategy for addressing the negative impact of Internet expression.

(ii) Enforcement response to change

This lack of volition by Parliament was not mirrored by a lack of objectionable expression circulating on the Internet; far from it. The Department of Internal Affairs had formed the Censorship Compliance Unit (the Unit), a team of inspectors established to detect and investigate objectionable publications and enforce the FVPC Act. With the advent of local online bulletin boards in New Zealand and the ensuing distribution of child exploitation images on those boards, the Unit began to investigate the Internet as a mode of offending. The Unit soon found the strategy of offenders was to figure out how to experiment with Internet

[143] Copyright (Removal of Prohibition on Parallel Importing) Amendment Act 1998.

[144] The Office of Film and Literature Classification *Annual Report* (1996) at 14.

[145] The Office of Film and Literature Classification *Annual Report* (1997) at 19.

[146] Russell Brown "Digital media and the internet - Law and regulation" (19 November 2014) Te Ara - the Encyclopedia of New Zealand <http://www.TeAra.govt.nz/en/digital-media-and-the-internet/>.

applications and products to see if it fitted their needs.[147] In the mid-1990s, ECPAT (End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes) called on New Zealand Police to send a representative to an Interpol-led meeting, the focus of which was child abuse and the Internet, but the national manager of the Unit was sent in their place.[148] At the time, New Zealand Police did not consider the Internet to be a significant issue for crime and enforcement.[149] However, in the UK, Operation Cathedral[150] had revealed "that offenders would very quickly use the Internet to facilitate the distribution of objectionable images" and on an international scale.[151]

The Interpol meeting was the impetus of the Unit's international cooperation measures. New Zealand inspectors trained with US enforcement agencies and developed formal and informal means of intelligence sharing to catch offenders. At other levels in government, strategies were also being developed to deal with the negative impact of Internet use. For example, in 1998 the Internet Safety Group had formed and their website *Netsafe* became a leading resource for New Zealanders. The Department of Child, Youth and Family Services, the Ministry of Education, the New Zealand Police and the Department of Internal Affairs also sponsored the Internet Safety Kit which was sent to every school and library in New Zealand in March 2000.[152] Thus in lieu of Parliament legislating on the issue, enforcement agencies (quick to see a need) interpreted their mandate broadly to accommodate the increasing impact the Internet was having on their enforcement role.

This loosely interpreted mandate proved useful for New Zealand's international cooperation strategy. The strategy became paramount as Internet offenders were not constrained by physical borders. As an example:[153]

> [New Zealand inspectors] were going on Internet Relay chat and we were getting a lot of Norwegians and because they [Norwegian law enforcement] couldn't target them themselves, they weren't allowed to go on internet relay chat, we would get the information for them … [European law enforcement] saw [it] as verging on entrapment. They didn't understand what we were doing. You were going into a public arena, but that took a long time to catch on.

---

[147] Interview with Steve O'Brien, above n 77.

[148] Above n 77.

[149] Above n 77.

[150] CNN "How police smashed child porn club" *CNN.com/World* (online ed, United States, 13 February 2001) at 1.

[151] Interview with Steve O'Brien, above n 77.

[152] Liz Butterfield *NetSafe: The New Zealand Model for Internet (ICT) Safety Education* (2000).

[153] Interview with Steve O'Brien, above n 77.

This was a happy trade-off for the Unit thanks to the liberal interpretation of the Unit's powers under the FVPC Act. Part 7 of the FVPC Act sets out the search powers of inspectors. Defined broadly, s 108 allows for the unfettered seizure of objectionable publications. Additionally, search warrants are only required for "physical" places or things (such as computer hardware).[154] Non-private residences (such as public spaces) may also be entered if they are "open to the public".[155] Proceeding on the basis that the Internet is a public space, the Unit is not required to get search warrants to inspect communications made by parties online. As this policy has developed unperturbed by Parliament or the Judiciary it is now accepted practice.

While this liberal interpretation of the FVPC Act has enabled the Unit to exercise certain discretions, in other ways the Unit was and is entirely constrained by the statute. The Unit, since its inception, has always undertaken a "fly-fishing" approach when it comes to Internet activity: rather than monitoring all New Zealanders' Internet use, they find areas where illegal activity is taking place and target New Zealand based addresses.[156] As Internet applications developed with increasing sophistication, every time an application was targeted by enforcement, offenders would retreat into more secure spaces and experiment with new untargeted applications. The Unit was eventually able to resolve IP addresses to physical locations in New Zealand.[157] As law enforcement's technical capability improved, physical offenders lost the ability to anonymise themselves entirely: "offenders always open themselves up because as soon as you start trading in material you are giving away your addresses".[158] However if those addresses were not New Zealand addresses the Unit was not empowered to do much with them. Foreign parties could send objectionable publications to New Zealand to circulate with ease. Without direction from Parliament as to how to deal with these conditions, enforcement depended entirely on (mostly) informal cooperation if they wished to target such offenders.

(iii) Industry response to change

By 2001, 47 percent of New Zealand households had a home computer, and 37 percent of households had access to the Internet.[159] The OECD reported at the time that New Zealand had one of the highest penetrations of secure servers amongst OECD countries, with users

[154] Films, Videos, and Publications Classification Act, ss 109 and 109A.

[155] Films, Videos, and Publications Classification Act, s 106.

[156] Interview with Steve O'Brien, above n 77.

[157] Above n 77.

[158] Above n 77.

[159] Statistics NZ *Information Technology Use In New Zealand 2001* (Wellington, 2002) at 11.

spending on average 30 hours online per month.[160] ISPs were enjoying this upsurge and faced little competition because of loop bundling (Telecom owned most of New Zealand's telecommunications infrastructure at the time).

At the turn of the millennium, Parliament had still not addressed the impact of the Internet on censorship law, had not investigated the role upstream parties played in Internet transactions, and had not responded to the increasing convergence and vertical integration of services. On the issue of convergence and the potential harms of unregulated expression, ISPs were reticent, concerned with growing the market instead of regulating it. Telecom's Chief Operating Officer commented:[161]

> Until a critical mass of New Zealanders use broadband on a daily basis, and experience firsthand how it can enhance their lives – convergence will just be a lot of hot air … From now on, our focus will be on providing content and services tailored for the broadband environment in an integrated way.

ISPs would maintain they had no role in the regulation of the Internet, and would insist on being exempt from any regulation that did take place. Individuals were targeted instead of upstream network or service providers.[162] While Parliament was beginning to acknowledge the issue of Internet-enabled crime, there was little attention paid to the broader structural climate that promoted this crime. In the short history of the FVPC Act, ISPs managed to entrench the ideology that that they should be exempt from any liability for offending online and from the burden of classification enforcement. Section 25 of the FVPC Amendment 2005 made special exemption from liability for "network operators" and "service providers". An assumption reigned that providing access to a service, regardless of whether that service facilitated criminal offending, should not attach liability to the service provider. By way of comparison, the Copyright (New Technologies) Amendment Bill had proposed that ISPs must adopt policies to terminate accounts of repeat offenders[163] but after heavy opposition from ISPs, this section was withdrawn and the subsequent 2008 Act made no such reference to ISP liability.

---

[160] OECD *The Development of Broadband Access in OECD Countries* (DSTI/ICCP/TISP(2001)2/Final, 29 October 2001) at 29.

[161] Simon Moutter "Making convergence a reality" (Telecom press release, 4 April 2003).

[162] For instance, the Crimes Amendment Act 2003 introduced "crimes involving computers": Crimes Amendment Act 2003, ss 248–254.

[163] Copyright (New Technologies) Amendment Bill 2008, s 92A(1).

During this period, Parliament only intervened in the market for Internet services in order to stimulate competition, hoping to increase New Zealanders' access to the Internet. In 2006, the New Zealand government announced plans to unbundle the local loop in New Zealand, in line with OECD recommendations. Telecom was forced to allow third parties access to its infrastructure on a non-discriminatory basis. This led to the swift uptake of broadband services and so by the end of 2006, one third of New Zealand homes had broadband access, with the largest demographic of Internet users being 15-24 year olds.[164] Meanwhile, the telecommunications industry has enjoyed and continues to enjoy billions of dollars of government spending on infrastructure.[165]

(iv) Attempts at substantive amendment

The government's response to this change and the interpretative challenges it posed to censorship law was not to inquire as to whether the language of the statute was neutral enough to apply to new technology and in such a way that was clear and certain, but to layer reactive and cosmetic amendments upon the original version. Since its enactment the FVPC Act has been amended seven times.[166] And despite these amendments, the substance of the FVPC Act has remained largely intact. This is qualified only by the rights jurisprudence which changed the way in which the Classification bodies undertook their duties and reflected the changing dynamic between states and citizens (as filtered through the courts) without alerting Parliament to the need to review the statute.

DVD finally matched video numbers submitted to the Classification Office by 2004.[167] When the interpretative issues with the FVPC Act became impossible to ignore, in March 2003 a report from the Inquiry into the Operation of the Films, Videos, and Publications Classification Act 1993 was tabled raising a number of concerns such as:

- "…'grey areas' in the censorship, and classification of publications";[168]
- "…how much objectionable material is going unchallenged in New Zealand";[169] and

[164] Statistics New Zealand "Household Use of Information and Communication Techonology: 2006" (27 April 2007) <www.stats.govt.nz>.

[165] Ministry of Business, Innovation and Employment "Fast Broadband" (11 December 2015) <www.mbie.govt.nz >.

[166] The first in 1997 was a mere formality: it made four amendments that repealed the transitional regulations. The next amendment, in 1998, replaced a section to make Ministerial appointments of censors simpler and easier.

[167] The Office of Film and Literature Classification *Annual Report* (2004) at 45.

[168] Government Administration Committee *Inquiry into the Operation of the Films, Videos, and Publications Classification Act 1993 and related issues* (March 2003) at 19.

[169] At 29.

- "…inconsistency between the various sectors of the industry serves to undermine industry confidence in the censorship regime provided by the Act and confuses the general public".[170]

The report made 34 recommendations. A new Bill was introduced in December 2003 to address the wider concerns around the operation of the FVPC Act. The aim of the Bill was to:[171]

> …address changes that have occurred in the nature and scale of offending, particularly in relation to the distribution of child pornography on the Internet. The Bill also clarifies aspects of existing classification criteria and makes changes designed to improve the practical operation of the Act.

The Government Administration Committee reported back in August 2004. They recommended the scope of the FVPC Act should be left undisturbed:[172]

> Any limitation, however, on the freedom of expression should be clearly defined and deliberately considered. Rather than expand the scope of the censorship law generally, the bill as introduced focuses on tailoring appropriate solutions to identified problem areas.

Crown Law, on behalf of the Attorney-General, finally indicated that there were prima facie inconsistencies between the FVPC Act and the right but that there were "sufficient procedural restrictions" in the amendment to mean that the Bill would not be inconsistent with NZBORA.[173] Other recommendations included not enacting separate "child pornography" offences[174] and exempting ISPs from liability if they did not have the requisite mental elements.[175] Such recommendations signalled a changing awareness about the impact of the Internet. Many recommendations of both the Inquiry report and the Select Committee report were ignored and/or dismissed. The resulting Films, Videos, and Publications Classification

---

[170] At 49.

[171] Supplementary Order Paper 2005 (325) Films, Videos, and Publications Classification Amendment Bill 2003 (91-1) at 1.

[172] Films, Videos, and Publications Classification Amendment Bill 2003 (91-2) (select committee report) at 2.

[173] Crown Law *Legal Advice Films, Videos and Publications Classification Amendment Bill Consistency With The New Zealand Bill Of Rights Act 1990* (14 November 2003).

[174] Supplementary Order Paper 2005, above n 174, at 7.

[175] Supplementary Order Paper 2005, above n 174, at 8.

Amendment Act 2005 made 38 amendments to the FVPC Act.[176] This set of amendments has been the most substantive to date, and whilst it provided some solutions it provided no vision for the future of censorship law and its application to the Internet.

Amendments to the FVPC Act in the subsequent years have been similarly cosmetic. A 2012 amendment that purported to modernise the statute was purely economic, addressing the cost of maintaining the censorship regime (which was borne largely by the government). Speaking to the Bill, Sam Lotu-Iiga MP said, "this will reduce compliance costs by an estimated $1.3 million next year, and that figure will rise to $2 million per year by 2018".[177] This obviously did not address the deep-seated issues with the statute's text, the justifications for continued state censorship or the systematic conditions that made compliance and enforcement difficult and costly.

(v) An ideological shift

Child sexual exploitation would become the locus around why continued state censorship was justified and necessary, deflecting attention away from all other harmful expression and the role of the state in regulating it. In 2008, the Unit developed a filter called NetClean and began trialling it with ISPs. ISPs eventually began to implicate themselves in Internet enforcement practice, formally in the case of copyright law and informally in the case of censorship.[178] Despite the FPVC Act dealing with all manner of expression that causes injury to the public good, the only material that was subject to the NetClean filter was obvious child abuse material. This was seen as a means of assuaging ISPs fears about broad unjustified censorship.[179] After the trial, the majority of ISPs agreed to implement the filter. Orientating censorship around the issue of child sexual exploitation was met with little industry and public resistance. New Zealand Police were also urged to take on an enforcement role, another by-product of the child sexual exploitation emphasis, and formed the OCEANZ (Online Child Exploitation Across New Zealand) team in 2009.

This subtle ideological shift would have enduring impact on the normative weight of the law, particularly those parts of the law that do not deal specifically with child sexual exploitation,

[176] These included adding ss 3A and 3B, replacing definitions such as "films" with "publications" and expanding the meaning of "electronic", updating offences including the "with knowledge" offences, clarifying review procedures and labelling body requirements and introducing new procedures for obtaining search warrants.

[177] (23 August 2012) 683 NZPD 4757.

[178] In the area of copyright law, the Copyright (Infringing File Sharing) Amendment Act 2011 created a special regime for ISP enforcement of copyright.

[179] Interview with Steve O'Brien, above n 77.

discussed later in this thesis. To this end, the Ministry of Justice reported in 2012 that the Internet was having a significant impact on the trade of child exploitation publications. They noted that "[t]he content of the publications is getting worse and that the children are getting younger … Despite these trends, sentences for child pornography related offending are generally well short of the maximum penalty available."[180] They also highlighted the limitations of the FVPC Act: "As the Classification Act relates to publications, in order to establish an offence against the Classification Act a record of the communication must be deliberately kept by the offender (i.e. a publication made)."[181] Technologies were being used in such a way that did not always leave records of the publication/communication and people could easily view objectionable material without ever actually possessing it (this was a problem because possession is one of the core offences of the FVPC Act).[182] The report made a number of suggestions for improvement.[183] Parliament deferred most of the issues raised by the Ministry of Justice.

It was not until the most recent 2015 amendment that some life was given to a small number of the Ministry of Justice's recommendations.[184] Most interestingly, s 131 was amended to state:[185]

> that a person can have an electronic publication in that person's possession for the purposes of the offence even though that person's actual or potential physical custody or control of the publication is not, or does not include, that person intentionally or knowingly using a computer or other electronic device to save the publication (or a copy of it).

Speaking to the Bill, the Minister of Justice said:[186]

> Advances in technology mean that offenders with exploitative intent can now communicate with children with ease. These indecent communications with young people

[180] Ministry of Justice *Regulatory Impact Statement: Addressing Child Pornography and Related Offending* (Wellington, 2 August 2012) at 4.

[181] At 4.

[182] At 5.

[183] Such as, the leave of the Attorney-General to bring a prosecution under the Classification Act is no longer serving a useful purpose, that it "may be desirable to combine an increase in statutory penalties with other measures to discourage child pornography and other related offending" and "to create a new offence in the Crimes Act of indecent communication with a child".

[184] The Act increased maximum penalties, created a presumption of imprisonment for repeat child pornography offenders, removed the Attorney-General's leave requirement for public prosecutions of offences.

[185] Films, Videos, and Publications Classification Act 1993, s 131(2)(A).

[186] (2 April 2015) 704 NZPD 2891.

> can occur in a variety of old and new media including text and picture messaging, internet chat, and telephone, and a specific offence is needed to ensure that this damaging behaviour is criminalised regardless of how it occurs.

Dissenting comments were made by the opposition:[187]

> But this legislation does not—and this is, I guess, our main problem with it—fit into an overall strategy for dealing with objectionable material generally; that is, child exploitation, cyber-bullying and abuse, particularly online, which is affecting and also perpetrated by children … Therefore, with all of these pieces of legislation, there needs to be a wider look at how they fit within a wider strategy.

Such comments appropriately summarise the current regulatory strategy in New Zealand, one that is less developed and inert compared to other comparable countries. This latest amendment may have modernised the FVPC Act with respect to issues such as possession and penalties, but does not address enduring concerns about censorship, such as the changing climate or the future of the right to freedom of expression.

C A Sample of defective aspects of the FVPC Act

The nature of drafting is such that there will always be limitations to the language of many statutes which undermine their adequacy in certain ways. However, the inattention this particular statute has received from the public, lawmakers, and other stakeholders has meant that the law has become disconnected from its purpose. When addressed, it has suffered cosmetic amendment and poor judicial interpretation. The current legal framework thus risks subjecting New Zealanders to injudicious outcomes. Furthermore, while it is always hoped that law will develop incrementally and in principled ways, such aspirations have been disrupted by the Internet. Technologically deterministic law also becomes rapidly irrelevant as technology inevitably changes. The weaknesses and inadequacies of the statute means that the FVPC Act risks being unfit for purpose in the event of any immediate change to Internet technology. This is most overt in the case of the definition of publication and in the offence provisions of the statute. Firstly, the law is now unintelligible to lay New Zealanders and does not reflect their online experience. Secondly, the state of the law is such that if enforced more strictly many New Zealanders would likely fall foul of it. The mere use of a certain technology should not lead to criminal liability for some and exemption for others (implicating the right to freedom of expression).

---

[187] (2 April 2015) 704 NZPD 2891.

This section will also set out how a class of service providers are now exempt from liability because the state has failed to reflect on the role and legal responsibilities of this class. Any attempt at state regulation of these private entities in the future will make the state more overtly censorious, which will have implications for the right to freedom of expression. Given these private entities' importance to the future of expression, this is a significant oversight. The issue of jurisdiction and extraterritoriality and the lack of clarification on these matters has undermined the adequacy of the FVPC Act. For those attempting to enforce the FVPC Act, this has meant coming up with creative ways to engage in their duties, shrinking their mandate in some respects (because of concerns over liability and jurisdiction) and exceeding it in others, potentially in a rights-inconsistent way. That the Unit's enforcement work is undermined because of limitations in the statute is problematic, particularly when this has little to do with preventing the state from acting unjustifiably and more to do with the lack of a coordinated regulatory conversation. This thesis argues that a natural outcome of the status quo will be the ceding of law-making authority to other jurisdictions or to private entities. In either case the practical burden of regulating expression will be placed entirely on New Zealand users. This will overwhelm the vertical rights relationship between the citizen and the state.

1 The difficulty with defining the term "publication"

The censorious state must define the form of expression it seeks to censor. A definition traps the expression into a legal concept able to be understood and adjudicated upon. The FVPC Act does not legislate in respect of all forms of expression. The FVPC Act is concerned with "publications" and the expression therein. In order to understand what expression the FVPC Act relates to and thus how it restrains expression, it is necessary to first understand what a publication is.

Section 2 of the FVPC Act states that that "publication" means:

> (a) any film, book, sound recording, picture, newspaper, photograph, photographic negative, photographic plate, or photographic slide:
> (b) any print or writing:
> (c) a paper or other thing that has printed or impressed upon it, or otherwise shown upon it, 1 or more (or a combination of 1 or more) images, representations, signs, statements, or words:
> (d) a thing (including, but not limited to, a disc, or an electronic or computer file) on which is recorded or stored information that, by the use of a computer or other electronic device, is capable of being reproduced or shown as 1 or more (or a combination of 1 or more) images, representations, signs, statements, or words.

Basic statutory interpretation principles would suggest that this list is exclusive (i.e. that any form of expression not stated here are not covered by the FVPC Act). This is the first step in drawing boundaries around the boundless concept that is expression. Many of the items within the definition will be plain and clear to the ordinary person. However, this definition is located in a cultural and historical context, one limited by the technology available to individuals at the time of drafting. Many people born after the introduction of the FVPC Act may not know what photographic negatives, plates or slides are. This demonstrates the primary tension in drafting a law that is precise enough to be capable of being easily understood by others but is also capable of being flexible to change. It is clear now that the language used is overly technologically deterministic and this is, in part, a reason for the ensuing interpretative difficulties.

There is a specific separation between subsections (a) and (d), the first three of which require a publication to have tangibility. The items described, films, books, images on paper, are all physical things with physical attributes. They are not thoughts, abstract or transient. However, a distinction is then made between these and "things" including electronic or computer files (subsection (d)). This is where the definition takes on a more abstract quality. Subsection (d) is plainly capable of broad meaning, potentially capturing all stored digital expression. This is qualified by the fact that a publication must be capable of being submitted to the OFLC and examined.[188] This naturally excludes live performances such as public speeches or theatre and reflects the practical needs of prior restraint. The "thing" must be capable of being reproduced or shown and suggests that a degree of permanence is necessary. McCarthy believes that the practical effect of the s 2 wording is that any digital media may be regarded as a publication under the FVPC Act.[189] Given the vast quantity of digital media, it is worth exploring whether there are any further qualifiers on what is capable of being a publication.

It may be of no surprise that broadcasting is absent from the list in s 2. Broadcasting is:[190]

> any transmission of programmes, whether or not encrypted, by radio waves or other means of telecommunication for reception by the public by means of broadcasting receiving apparatus but does not include any such transmission of programmes—
> (a) made on the demand of a particular person for reception only by that person; or
> (b) made solely for performance or display in a public place

[188] Films, Videos, and Publications Classification Act, s 23.

[189] Miles McCarthy "Censornet: The Competing Ideals of Censorship and Cyberspace" (1997) 27 Victoria U Wellington L Rev 349 at 352.

[190] Broadcasting Act 1989, s 2.

Put simply, broadcasting is where the public receives transmission of programmes. There have historically been strict distinctions between the jurisdictions of the FVPC Act and the Broadcasting Act 1989. In some ways, broadcasting is akin to live performance, with much of broadcast programming aired live. To reiterate, this affirms the permanence necessary for publications, as stated by previous authors[191] and as understood by the OFLC:[192] as no record exists after a broadcast, whatever was broadcast cannot amount to a publication. Put another way, as the programme cannot be reproduced or shown (as the broadcast has ended), it cannot be a publication. The separation is further maintained by s 4(2) of the Broadcasting Act 1989, which requires the consent of the Chief Censor if a broadcaster wishes to broadcast an objectionable film. However this leads necessarily to the conclusion that a broadcast recorded or stored before or after the act of transmission is capable of being a publication. Thus, while the definitions are independent they are not mutually exclusive. Subsection (a) further stipulates that it is not broadcasting where an individual seeks out a programme rather than having the programme passively delivered to them via transmission. If an individual can "pull" or choose the programme self-selectively, this act must be underscored by the fact that the programme is stored and is therefore a publication. This fact results in an overlap between the definitions of a broadcast and a publication and thus an overlap in jurisdiction.

A similar comparison can be drawn between the definition of a publication and the definition of a "digital communication" found in the Harmful Digital Communications Act 2015. A digital communication:

> (a) means any form of electronic communication; and
> (b) includes any text message, writing, photograph, picture, recording, or other matter that is communicated electronically.

Ultimately, a publication may be an electronic communication, but an electronic communication is not inherently a publication for the purposes of the FVPC Act. In summary, the circumstances in which the expression in question is made available and endures determines whether or not it comes within the ambit of the FVPC Act.

---

[191] Cheer, above n 5, at [10.3.2(a)].

[192] Office of Film and Literature Classification "Classification In New Zealand" (8 April 2015) <http://www.classificationoffice.govt.nz/about-censorship/new-zealands-censorship-law-the-films-videos-and-publications-classification-act-1993.html> .

The court has also gone some way towards clarifying the meaning of publication. In *Goodin v Department of Internal Affairs*, O'Regan J stated:[193]

> It will be a matter of election as to whether the publication which is the subject of classification, or the subject of a charge under the Act, is the individual picture or photograph or the book or magazine.

O'Regan J held that a computer hard drive, or the individual images or .jpeg files (an electronic format for images) it contained, could each be publications for the purposes of the FVPC Act. Whilst s 2(a) only applies to physical photographs,[194] he stated that a "picture" is capable of meaning a digital image for the purposes of s 2(d).[195] He also affirmed that folders and files are capable of meeting the subsection (d) definition.[196] In doing so, O'Regan J affirmed the definition set out in *Department of Internal Affairs v Merry*[197] and *R v Millward*,[198] where "computer pictures" and "computer files", respectively, were considered to be capable of being publications for the purposes of the FVPC Act.[199] The decision acknowledges that while some publications do not neatly fit into any particular subsection (and there will be overlap), strict demarcations could undermine the FVPC Act's purpose. A degree of common sense is necessary when determining whether something is a publication.

The courts have also grappled with whether there are certain elements of a thing that go to its capacity to be a publication:

(a) In *G (CA741/11) v R*, Simon France J rejected the Crown's argument that the whole computer was a publication (for the purposes of obtaining a warrant under s 108 of the FVPC Act), using subsection (d) to draw a distinction between devices and files. He suggested that describing a computer as a publication "as opposed to being the means by which publications may be displayed" was discordant with ordinary usage.[200] This distinction has some utility in further narrowing what exactly a publication can be.

---

[193] *Goodin v Department of Internal Affairs* [2003] NZAR 434 (HC) at [30].

[194] At [36].

[195] At [38].

[196] At [42].

[197] *Department of Internal Affairs v Merry* [2000] DCR 733.

[198] *R v Millward* [2000] DCR 633.

[199] *Goodin*, above n 193, at [29].

[200] *G v R* [2012] NZCA 152 at [21].

(b) Chisholm J, in *Kellet v Police*, stated that s 2 is a wide definition and "does not distinguish between different modes of communication".[201] The Court suggested that the copying of information from a hard drive to CD Rom and then between CD Roms did not affect the information's capacity to be a publication.

(c) *R v Schaper* set out that a stored image which is recovered (in this case by the Department of Internal Affairs using a forensic recovery program on computer hardware), is capable of being "a thing" covered by the s 2(d) definition.[202]

(d) It was argued in *R v Spark* that the publications (text files on the defendant's computer) were not publications for the purposes of the FVPC Act because the appellant did not intend to make them available. The Court of Appeal held that the definition of a publication "contains no requirement of availability, nor does it even hint at such a requirement".[203] The Court also rejected the notion that the state of mind of the person making the publication is relevant to whether or not it is a publication.[204] The Supreme Court did not disturb this finding on appeal.

This case law suggests that whilst it is important to maintain some conceptual distinctions in the s 2 inquiry, the section intends to covers a wide variety of expression irrespective of the intention of the maker of the publication and the platform used to make and make available the expression, subject to the qualifications already discussed. The result is a wide and inclusive definition that may lack the precision necessary for ordinary individuals to anticipate whether or not they are dealing with a publication for the purposes of the FVPC Act (in some part because of the overlap with other statutorily defined forms of expression).

There are unresolved issues as to whether expression communicated via streaming and peer to peer technology are publications. This was anticipated during the 2004 inquiry into the classification scheme by the Government Administration Committee. As a result of the inquiry and subsequent amendment to the FVPC Act, there lies a definition of digital content, buried in s 122A of the FVPC Act. Digital content "means information that is kept on a data storage device and accessed, or available for access, through a public data network; but (b) does not include email, or information that is transmitted in the form of a broadcasting service". Section 122(1)(b) suggests digital content "is or includes the publication". It is thus clear that

[201] *Kellet v Police* (2005) 21 CRNZ 743 (HC) at [21].

[202] *R v Schaper* DC Christchurch, 21 April 2008.

[203] *R v Spark* [2009] NZCA 345, 3 NZLR 625 at [25].

[204] At [25].

Parliament intended as early as 2004 that the definition apply to the Internet in some way (although streaming technology specifically was yet to be popularised).

Enduring debate on this interpretative issue (whether publication applies to online expression) merely distracts from other more pertinent issues and contributes to the law becoming impractically technologically deterministic. However, for the sake of argument, it is worth exploring whether the expression enabled by these technologies is capable of amounting to a publication. When information or data is downloaded onto a person's device, a copy of that data now exists as a file on that person's device. The data exists at the point of origin and at the point of reception, and is capable of being recovered at both points. This data fits comfortably into the definition of a publication. Compare this to when a program plays a streaming file. Streaming involves information requested by the user then being displayed or rendered as it is transmitted in real time to the device. The data is not copied onto and stored on the user's device. The program, instead, discards the data in real time as a viewer watches it. The streaming file exists at the point of origin but not at the point of reception, only capable of being recovered at the point of origin. *R v Schaper* suggests that when considering whether information is capable of being a publication, the most important question appears to be whether or not the information is capable of being recovered. Streamed data cannot be recovered from the point of reception, so may lack the necessary features of a publication (if point of reception was the only consideration). However, the data still exists at, and can be recovered from, the point of origin; it therefore amounts to a publication at that point of origin. In any case, if data exists on a server or device and can be reproduced or shown, the fact that it is later streamed (and the data is discarded at the point of reception) does not impact on its capacity to be a publication.

The above point is complicated by the fact that there are distinctions between streaming services. Applications like YouTube use Over-the-Top-Technology (OTT) unicast streaming, meaning every individual user gets their own stream of data delivered to them. By contrast, other on-demand services may use Internet Protocol Television (IPTV), where a closed network is managed by a party using online transmission technology and delivered to members of the network simultaneously and as they request it. This may lead to the assumption that OTT streamed data is more synonymous to a broadcast rather than a publication. This author disagrees. Such demarcations would amount to imputing highly precise boundaries into the definition of a publication and also the definition of a broadcast under the Broadcasting Act 1989, largely undermining Parliament's intention and the longevity of both statutes. Drawing upon the principle of functional equivalence, it is only where the activity is not equivalent to the previous one where a new "rule-set" or law needs to be made. The purpose of the FVPC

Act is the prevention of injury to the public good via the availability of certain types of expression contained in publications. While the definition of publication has its limitations, for reasons already highlighted, it is not so poorly drafted that it cannot apply to digital media and new media technology as it emerges. There is room for improvement (explored later in this thesis) however it is not correct to make strict technological demarcations when interpreting what a publication is, unless this definition is to become so precise that it cannot capture expression that is likely to cause injury to the public good. It would also suggest that it was Parliament's intention to amend the FVPC Act every time a new technology emerged, which is not only unlikely but impractical from a drafting perspective. Ultimately, this wrangling of definitions obfuscates the purpose of the FVPC Act and is likely to result in arbitrary and injudicious applications of the respective statutes (which burdens the right to freedom of expression) and a gap in jurisdiction where likely injury transpires (undermining the purpose of the law).

2 FVPC Act offences

After finding that a publication is objectionable, it must be determined whether what has been done with that publication is criminal. The freedom for an individual to act with an objectionable publication is regulated by the offences described in Part 8 of the FVPC Act. It should be noted that s 124A and s 128 set out miscellaneous exceptions to these offences, but they are not relevant for present purposes. The offences under the FVPC Act are a mixture of strict liability and fault-based liability offences. Naturally, the fault-based liability offences come with more severe consequences for the offender. Given the gravity of the matter of criminalising expression, these offences should at least be legally knowable to an individual so as not to amount to an undue burden on the individual and their right to freedom of expression. The application of these offences should aspire to be clear and precise. However, as the following discussion will highlight, the language of these offences has not stood up to the test of time. Further, the qualities of clarity and precision have declined as the case law on these offences has developed.

(i) Possession

It is an offence to "possess" an objectionable publication:[205]

> every person commits an offence against this Act who, without lawful authority or excuse, has in that person's possession an objectionable publication.

[205] Films, Videos, and Publications Classification Act, s 131(1).

Section 131(3) states it is no defence that the defendant had no knowledge or reasonable cause to believe that the publication was objectionable. There is a harsher penalty where the defendant had knowledge that the publication was objectionable (s 131A). One author has claimed that strict liability attached to the possession offence is contrary to the rule of law and the NZBORA, calling for its repeal.[206] Given the development of the law and the changes in technology, these concerns are not exaggerated. Judge Harvey poses a hypothetical where a "naïve" computer user browses the web, comes across an "extreme" site, quickly exits the browser but later cached images from the site are found on his computer. He suggests that this "innocent curiosity can lead to a charge of a serious offence".[207] The issue has been considered at length by the courts. What does it mean to possess something, particularly as this possession amounts to a strict liability offence? The following discussion of the historic precedent informs the current position on possession which, due to recent amendment, may also amount to the mere viewing of objectionable publications.

Judge Henwood, in *Department of Internal Affairs v Merry*, set out four essential elements for a charge of possession to be satisfied.[208] The first is that the defendant had actual or potential control over the item; in *Merry* the defendant controlled the system and was the only person able to delete the items. The second is that the defendant knew what he had control over; this does not have to be precise but a person cannot possess something if they do not know what it is. This is not the same as a requirement that the defendant know that what they possessed was an objectionable publication. The third is that it must be shown that the defendant has the intention to exercise control. The fourth is that the possession was voluntary and not forced or coerced. This reasoning was later affirmed in *Goodin v Department of Internal Affairs*, *Department of Internal Affairs v Young* and *Meyrick v Police*. However these later decisions have expanded upon this reasoning.

Whilst conceding that proving knowledge that a publication is objectionable is not an element of the offence, O'Regan J in *Goodin* emphasised that "proof of possession requires proof of some element of knowledge".[209] He was not satisfied that the mere presence of an objectionable publication on a hard drive amounted to possession. A prosecutor would have to prove that the defendant had knowledge that he was in possession of a publication. In finding that there needs to be a deliberate intention to possess a publication, the Court confined one

[206] Dean Knight "Objectionable Offence: A Critique of the Possession Offence in the Films, Videos, and Publications Classification Act 1993" (1997) 27 VUWLR 451 at 487.

[207] Harvey, above n 122, at [4.11.2].

[208] *Merry*, above n 197.

[209] *Goodin*, above n 193, at [19].

aspect of the strict liability element of the offence. What remains is that it does not matter whether a defendant knows the publication is objectionable or not objectionable.

Department of Internal Affairs v Young dealt with the issue of whether, having opened and viewed the publications (knowing what he would see) then having closed them, the defendant could be in possession of the publications. Judge JE Ryan could not see any logical reason why "consciously saving an objectionable publication to a file, a disk or printing or dealing with the publication in any other way, is a necessary ingredient of possession".[210] He considered that the image being tangibly present on the computer screen amounted to possession. The defendant having sought out the publication "had full control of it although the exercise of that control was limited to accessing, opening, viewing and closing the publication".[211] *Young* established that possession can be fleeting. It was sufficient that Mr Young had, at one point in time, the ability to control what appeared on his computer screen. Possession, thus, can be something less than holding onto the publication indefinitely.

The High Court decision of *Meyrick* (whilst affirming these previous decisions) did qualify possession somewhat. Nicholson J endorsed the following reasoning of the lower court:[212]

> What has specifically troubled me in this regard, having regard to considerations of public policy in this troublesome area—as I earlier pointed out to the parties—is that for an ordinary layman, and I class myself in this capacity, if objectionable material is received on one's personal computer as all too often regrettably it is in these days of spam and other practices, the only reasonable steps it seems to me that the average person could take, is to highlight and delete those files, and then take the second step of emptying the waste disposal, or 'trash bin'. Most ordinary computer users would, I am sure, consider that they had, by those steps, made the images effectively unrecoverable, and unless it was shown that by some further step the defendant had, having taken those steps, or having had those steps taken for him, somehow subsequently, and within the period of two years prior to the laying of the informations, exercised some effective control, thus demonstrating knowledge of those objectionable images, then it would be wrong in practice and in principle to find him guilty of 'possession' of them.

There is a sense of trepidation in Nicholson J's speech. He did not consider that voluntary and willing possession took place in the case of a person "who watches an objectionable image on a computer screen for only the short time that it takes to realise what it is, before removing

---

[210] *Department of Internal Affairs v Young* [2004] DCR 231 at [13].

[211] At [13].

[212] *Meyrick v Police* HC Hamilton CRI-2005-419-000058, 31 July 2007 at [172].

that image intending to put it out of their control".[213] It is this reasoning that undermines the validity of the concerns raised in Judge Harvey hypothetical. The law did not intend to trap such individuals and the common sense approach of judges has meant that this has not happened. That it is highlighted as an issue only in hypotheticals and counterfactuals shows that the law is working as intended in this respect.

In the case of *Batty v Choven*, the Court referred back to the plain meaning of possession established in *R v Cox*.[214] In line with the previous jurisprudence, Allan J held that the presence of objectionable material without knowledge did not amount to possession but was not sympathetic to "the viewing of objectionable material by someone who deals routinely in pornographic material" stating that this activity did constitute possession.[215] In this case:[216]

> [t]he applicant knew perfectly well that the images, although deleted, remained within his control, and would remain so until either he took a further overt step, or the images were automatically over-written. In those circumstances the claim that the applicant nevertheless did not intend to view the images in the future, was beside the point. They remained his possession.

Although alive to the issues put forward by Nicholson J, Allan J appeared to be less haunted by the spectre of innocent men stumbling around on the Internet, having to dodge the endless array of child sex abuse potholes.

Although the case of *R v D* concerned the legality of a search warrant, the issue of possession was also considered. Justice Heath considered that the concept of possession must be addressed with "some care".[217] He was concerned that in the case no evidence was produced to prove that the holders of the respective IP addresses had actual or potential control over the images; that no evidence demonstrated that they had reasonable cause to believe that the images were objectionable; and that there was no information as to how long the link was open for, whether it was saved to a file, or whether it was deleted or double deleted in order to demonstrate belief or knowledge that what they possessed was an objectionable publication.[218] This goes some way to understanding what judges consider the threshold to be for proving possession but this should not be taken as the accepted approach to possession. The jurisprudence highlights an ongoing (seemingly invalid) concern for "innocent" viewing and

---

[213] *Meyrick v Police*, above n 212, at [179].

[214] *R v Cox* [1990] 2 NZLR 275 (CA).

[215] *Batty v Choven* (2005) 23 CRNZ 214, [2006] NZAR 127 at [10].

[216] At [10].

[217] *R v D* [2011] NZCA 69 at [63].

[218] At [67].

how it should factor into an understanding of possession. The courts have imputed knowledge or deliberateness into the actus reus, that is, in the act of taking possession of the publication. However, knowledge that the publication is objectionable is, and has been, a requirement of the offence.

(ii) Mere Viewing

Parliament further legislated on the issue of possession. The introduction of the Films, Videos, and Publications Classification (Objectionable Publications) Amendment Act 2015 intended to clarify, once and for all, that possession of objectionable electronic publications includes viewing the material without intentionally or knowingly downloading it or saving it (s 131(2A)). This amounts to a negative addition to the offence rather than expanding it and may have been somewhat superfluous in light of *Young*. Returning to Judge Harvey's hypothesis, it is plainly unlikely that a successful prosecution could be mounted against his "innocent" defendant. The "mere presence" of cached images on his hard drive will be insufficient, unless the prosecution could prove he viewed the images or knew the cached images were on his hard drive. Further, they would need to prove that he had the knowledge and capacity to retrieve the images and thus demonstrate control. The legislative amendment is unlikely to alter this position. In coming across an "extreme site" and having quickly exited the browser, a defendant is unlikely to surmount Nicholson J's threshold for voluntary and willing possession. Something more will be needed such as in the case *Batty v Choven*, where it could be proved that the defendant was a regular viewer of objectionable material. The knowledge and control requirements set out in *Meyrick* are likely to have utility in this regard and it is foreseeable that a court will reiterate that the knowledge and control requirements still apply even where the publication is not downloaded or saved.

Despite the legislative amendment, intended to clarify the law and reflect the modern online experience, the possession offence is becoming more complex rather than less. Furthermore, if the law becomes overly technologically deterministic in this respect, there is a risk it will quickly fall behind the technology (requiring frequent amendment) and thus lose its utility. Mere viewing of objectionable publications (without downloading or saving) is now sufficient to amount to possession. The amendment has yet to be tested in the New Zealand courts but is likely to have implications for precedents set in cases such as *Meyrick v Police*.[219] The intention of the amendment is to capture offenders who are able to consume objectionable publications and escape liability by claiming that, because they did not save or download a file they were not in "control" of the publications (as discussed, a necessary requirement of

[219] Above n 212.

possession). Prior to the amendment, prosecutors faced difficulty in building cases against potential defendants as shown in the case of *R v Clarke* where the Court rejected the application for a warrant as the applicant failed to show that the alleged offenders had objectionable publications in their possession, only that they had accessed websites known to display objectionable publications.[220] Gillespie identifies that there are already a number of mere viewing offences in other comparable jurisdictions.[221] He highlights the example of the 2008 congressional amendment to the US Code which overturned many years of United States precedent with respect to viewing, knowing access now being sufficient instead of possession by control.[222] Thus the 2015 amendment to the FVPC Act is not without international precedent.

Mere viewing is a good example of how the internal versus external perspective theory can inform the interpretation of the law. Howard suggests that the difficulty with interpreting "viewing" offences is an issue of perspective. The law can target an individual's behaviour or the technology that enables it. Howard poses a conceptual challenge to courts: they must decide whether possession amounts to (a) what appears on the screen or (b) the contents of the defendant's cache, and then proceed to build analysis around this.[223] Howard believes that addressing what appears on screen rather than what is found in the cache more accurately reflects how the technology is used and will be a more sustainable position as the technology advances.[224] In the latter case, liability is incurred because copies of objectionable publications are automatically stored in a cache, not because a user seeks out and brings to screen objectionable content to view. The law becomes arbitrary when the substance of a case boils down to the issue of whether or not a defendant knows how a cache works.

The intention of the 2015 amendment was to close a loophole. However the text of the amendment speaks to "saving or downloading", these functions may become obsolete as Internet technology develops. Inevitably, if the law becomes affixed to technology, at any single point in its development, it is likely to stagnate. It is unlikely that New Zealand users would believe or appreciate, after reading the legislation, that by watching or viewing something onscreen that they have possessed an objectionable publication. This should be well-signaled to them if this is the case. It would be even more unpalatable to learn that deleting

[220] *R v Clarke* [2012] DCR 425 at 26.

[221] Alisdair A Gillespie *Child Pornography: Law and Policy* (Routledge, New York, 2011) at 186.

[222] Gillespie, above n 223, at 188.

[223] Ty E Howard "Don't Cache out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files" (2004) 19 Berkeley Technology Law Journal 1227 at 1253.

[224] Howard, above n 223, at 1272.

one's cache is a simple means to avoid liability. Caching is used to ease network congestion and should not trap innocent viewers or obviate the liability of deviant ones. Therefore it is difficult to conclude (a) that New Zealanders understand how this amendment will meaningfully apply to their Internet use and (b) that it will better ensure their compliance with the FVPC Act. In due course this overly technologically deterministic law may too cease to be relevant. The opportunity to amend the section should have gone further. In lieu of this, the longevity of this amendment will come down to how it is interpreted and applied.

(iii) Copying

A more compelling example of where there the text of the statute no longer bears relevance to the online experience is the copying offence provision. While there is copying in the physical world and on the Internet, the normative difference between the two is significant and not reflected in the statute. The New Zealand case law, in particular, demonstrates a lack of understanding about the technical properties of the Internet (including that copying is inherent in every Internet transaction) to the detriment of the law and those subject to it.

Section 123(1)(b) states it is an offence to make a copy of an objectionable publication for the purposes of supply, distribution, display, or exhibition to any other person. This offence functions well in a pre-Internet society, where an original publication and the copied publication can be physically differentiated from one another and identified as an original and a copy. The act of increasing the number of tangible objectionable publications is also normatively significant, such that it was appropriate to have a separate (and more serious) offence in relation to it. However, on the Internet this distinction disappears; indeed Mueller has described the Internet colloquially as a "gigantic, globally distributed, always-on copying machine".[225] To make a copy online has little meaning from a technical perspective as this is the basis of how the Internet functions (particularly the processes such as mirroring and caching). Gillespie highlights that even when viewing an image, "a temporary file is created on the device displaying the photograph" (this being a copy of the file from the server where it originated).[226] And as Reed has repeatedly stressed, copying is "fundamental to all communications between computers"[227] and it is "impossible" for a cyberspace user to consume content online without copying it. [228] Thus while the offence is still relevant to the

[225] Milton Mueller *Networks and States: The Global Politics of Internet Governance* (MIT Press, Cambridge (Mass), 2010) at 130.

[226] Alisdair A Gillespie "Jurisdictional issues concerning online child pornography" (2012) 20 Int J Law Info Tech 151 at 121.

[227] Reed, above n 75, at 14.

[228] Chris Reed *Making Laws in Cyberspace* (Oxford University Press, Oxford, 2012) at 155.

physical world where physical copies of publications are still made, it is of little utility to the offences of the FVPC Act when the Internet is concerned.

The decision of *Kellet v Police* highlights this misunderstanding and the danger of categorising certain online conduct into the s 123(1) offences without due consideration as to how the Internet is used. Chisholm J decided that consolidating material from various online sources into a folder constituted "making" an objectionable publication while downloading blocks of images from a hard drive onto CD ROMs constituted simple "copying".[229] In the latter instance, Chisholm J said "[the defendants] actions could be likened to the copying of a page or pages from a book for future reference".[230] Chisholm J uses functional equivalence theory to give life to the copying offence. However, with respect, the reasoning (a) misunderstands how the technology functions and (b) provides little guidance as to how different offences should be interpreted and applied to different types of conduct. Chisholm J justifies this with the assertion that every case will depend on its own facts.[231] In this case it is highly likely that the appellant's conduct would have been captured by the lower tier offending of s 131(1) of the FVPC Act. However it is also likely that the prosecution had a strong desire to pursue the more serious s 123(1) conviction (the text of which is reproduced in the following section of this thesis), but the prosecution's case did not meet the burden of proof for s 123(1)(b) (which includes the additional element of supply, distribution, display, or exhibition). Nonetheless, the prosecution's case was salvaged by his Honour's interpretation of "making" and its dubious differentiation from the "copying" offence. With respect, this is simply bad interpretation of the law. If the law continues to be applied in this way it will contradict and misconstrue the reality of many users' experiences online.

As it stands, the law is complex. An individual may possess an objectionable publication under s 131(1) by it being on their device, notwithstanding technically it must have been copied to the device for it to be on the device. However, if an individual deals with a publication by replicating its location within a device or onto another device this will amount to copying under s 123(1)(b). To then deal any further with the publication (for instance, to move it to a location where other publications are already located) would be to go beyond s 123(1)(b) and may even amount to the more serious s 123(1)(a) offending of making an objectionable publication. The margins that separate these actions from each other are so slight from a technical perspective that to be interpreted as legally different to one another is arbitrary and

[229] *Kellet v Police* (2005) 21 CRNZ 743 (HC) at 749.

[230] At 749.

[231] At 748.

superfluous to the purpose of the FVPC Act. Unfortunately, *Kellet v Police* is considered good authority for this application of s 123(1)(a).[232]

What these observations highlight is that the expression "to make a copy" cannot be technologically neutral and attempting to construe it as having application on the Internet is technically and legally problematic. What this instead represents is a scenario where there is no pre-Internet equivalent to assess the new activity against. Copying demonstrates the limitations of the statute's text and how these limitations prevent it from remaining relevant, particularly as the technology changes. It also highlights that though there is a desire by the court to be theoretically consistent (by always applying the principles of functional equivalence), it may not be conceivably or practically possible to do so. Attempts then to apply this law result in arbitrary outcomes.

(iv) Supply and Distribution

Supply and distribution are also strict liability offences in that knowledge that the publication is objectionable is not required. Likewise there is a harsher penalty where the defendant had knowledge that the publication was objectionable (s 124). Section 123(1) states:

> 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) imports into New Zealand an objectionable publication for the purposes of supply or distribution to any other person; or
> (d) supplies or distributes (including in either case by way of exportation from New Zealand) an objectionable publication to any other person; or
> (e) has in that person's possession, for the purposes of supply or distribution to any other person, an objectionable publication; or
> (f) in expectation of payment or otherwise for gain, or by way of advertisement, displays or exhibits an objectionable publication to any other person.

These subsections are of interest from a statutory interpretation perspective. The use of the semicolon and the word "or" suggest that the subsections are disjunctive. However, there appears to be overlap in the meaning of certain subsections, particularly because of the broad meanings of some of the terms used. Of course in the case of ambiguity, the surrounding subsections could aid in informing the interpretation of a particular subsection.

[232] The case was referred to in *Stewart v Department of Internal Affairs* [2014] NZHC 2209.

An example of this ambiguity is the overlap between subsections (b)–(e); each subsection uses the phrase "for the purposes of supply". This overlap confuses the plain meaning of supply to the lay person trying to understand what their conduct amounts to. Section 2 and s 122 inform s 123 by providing definitions of the terms "supply", "public supply" and "distribute". For instance, s 2 states that supply means to sell, or deliver by way of hire, or offer for sale or hire. By way of comparison, s 122 states that:

> (1) … *distribute*, in relation to a publication, means—
> (a) to deliver, give, or offer the publication; or
> (b) to provide access to the publication (for example, to provide access by means of a public data network to digital content that is or includes the publication).
>
> (2) However, a person does not distribute a publication unless the person—
> (a) intends, or knows of, the act of distribution; and
> (b) knows what, in general terms, the publication is or contains.

Section 122(3) qualifies this definition by stating:

> To avoid doubt, *to distribute*, in relation to a publication, does not include to facilitate access to the publication by providing only some or all of the means necessary for—
> (a) delivery of the publication in physical form; or
> (b) transmission (other than by broadcasting) of the contents of the publication.

And s 122(4) provides some examples to clarify the meaning of s 122(3).

Therefore, in the case of supply or distribution, it is an offence to offer a publication to another; however, if it is offered for sale or hire this more neatly fits within the definition of supply. If an individual offered the publication on some other pretence (such as non-financial gain), this conduct appears to more neatly within the definition of distribute. Drafters must have thought this distinction was necessary, although it not clear why from the statute text. If it was in the interest of covering all manner and range of conduct this could have been done with a broader term.

Section 2 and s 122 are therefore not particularly useful for making clear what types of conduct should be assigned to the particular offences. For instance, although to provide access to a publication is an offence (as it amounts to distribution), *facilitating* access to the publication by way of transmission explicitly does not amount to distribution. And the FVPC Act does not define the difference between providing and facilitating. The practical and normative

distinction between terms such as providing access and facilitating access, and supplying and distributing as forms of conduct seems negligible in the light of the broad range of conduct s 123 clearly intends to capture. If an individual sends a person a link to an objectionable publication, upon receipt of payment, it would seem counter-intuitive for the purposes of the FVPC Act that they should be absolved of liability because they are able to argue the semantic distinction of having merely facilitated access rather than having provided access to that website. There is no case law that deals specifically with this issue. Instead with offences involving the Internet, the offences put forward to the courts are inconsistent and indicate a lack of clear guidelines. In much of the reported case law there is little to indicate why supply versus distribute was chosen as the appropriate offence on the facts of the case. Judges have thus been forced to make distinctions that undermine the text of the statute. The most striking example is the term supply being read as implying an act of consideration (to distinguish it from the term distribute) leaving the *for gain* section of the statute meaningless.

Another vague drafting distinction is the use of "electronic" to define certain conduct. Section 123(4)(c) states that importing means not only physical importation but also "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". Importation is standalone in this regards. There is no reference to "electronic" supply or distribution, suggesting that "electronic" only applies to importation. The courts have rejected this (see *Millward* and *Benning* discussed below). This inconsistency is likely to be the product of the 2005 amendment that tried to capture Internet expression. Although attempting to imbue the principles of functional equivalence in the statute and redraft the sections to provide for the equal treatment of both electronic and offline activity, the drafters actually created inconsistent terminology. Vagueness as to why the term electronic was included (and what conduct it to apply to) has only led to inconsistency, undermining individuals' ability to make legal choices.

A further point to note is that whilst s 123 states that these are strict liability offences, s 122(2)(a) and (b) clearly implies knowledge into the meaning of "to distribute". This attribution of culpability mirrors what the courts have tried to achieve in relation to possession offending. That it occurs in the statute may simply be an issue of poor drafting or indeed a reflection of Parliament's intent that distribution requires a further dimension of culpability. The court's endorsement of this attribution of culpability is discussed below in the section on Liability under the FVPC Act.

Two judgments make significant inroads into how we should understand the function of ss 123 and 124. The first is *R v Millward*.[233] The accused had downloaded objectionable .jpg and .mpg files from internet newsgroups, sent them to other members of a newsgroup (as evidenced by his outbox) and then posted them electronically to another newsgroup. Judge M F Hobbs set out the elements for the offending under s 123(1)(b), (c) and (e). Whilst s 123(3) explicitly states it is no defence that the defendant had no knowledge or reasonable cause to believe the publication to which the charge relates was objectionable, the judge included "having reasonable cause to believe that the publications were objectionable" as an element of the offending in respect of all three charges. In relation to s 123(1)(e), he also included "for gain" as an element of the offence despite the fact that this term is not used in the text of this particular subsection. He did not provide reasons as to why "for gain" is included. The judge was satisfied, on the facts, that the accused had "distributed" the files by sending or posting the copies electronically, stating:[234]

> The Crown does not have to prove actual distribution of the material, only making copies of it for that purpose. However, if actual distribution is proved by the evidence, as is the case here, then of course the purpose is obvious.

By way of comparison, the judge was not convinced that this conduct amounted to supply as there was no valuable consideration for posting the files: "The statutory definition clearly envisages a sale for valuable consideration. It obviously envisages a transaction where there is a seller and a buyer."[235] On the issue of gain, the judge adopted the reasoning of Judge McDonald in *Department of Internal Affairs v Benning*[236] stating that "the word 'gain' should be not limited in these cases to monetary or other material gain" And further:[237]

> …The traffic in these publications presumably gives pleasure and some sort of satisfaction of those prurient interests to both those who distribute it and those who receive it. In my view, however one may regard the morality of the matter, that amounts to a "gain" by those persons having regard to the purpose of the statute creating the offence. If that were not sufficient, it seems to me that one has to have regard to the fact that the word "supply" is defined in the Act as meaning among other things "to sell". If distribution for "gain" meant simply to sell for monetary profit, then it would be superfluous to the purpose of s

---

[233] *R v Millward*, above n 198.

[234] At 5.

[235] At 7.

[236] *Internal Affairs Department v Benning* DC Dunedin CRN 7012018045, 12 March 1998.

[237] *R v Millward*, above n 198, at 10.

> 123 because the offence of supplying the publication would obviously include distribution of it for gain.

The Judge also dismissed the argument advanced by the defendant that the files needed to be distributed within New Zealand. Instead he found the recipient being "any other person" was without limitation in meaning, geographically or otherwise. This has important implications for the issue of liability and jurisdiction discussed in later sections of this chapter.

The second key decision was the decision of the High Court in *Shaw v Department of Internal Affairs*.[238] The appellant contested his conviction after he was found to have objectionable material on his home computer. The appellant also had Kazaa software on his computer, allowing him to share his files with others through a shared folder. Mackenzie J was unwilling to disturb the lower court's finding of fact that the appellant stored the material in the shared folder for the specific purpose of making these available to other persons in order that he obtain some gain.[239] Having set up the folder, knowing others could access it, and having loaded files into that folder was sufficient to have distributed those publications. Mackenzie J stated that there were five elements to be proved under s 124(1) (not referring to any particular subsection):[240]

(a) Making available;
(b) An objectionable publication;
(c) Knowing or having reasonable cause to believe the publication is objectionable;
(d) To any other person; and
(e) In expectation of payment, or otherwise for gain.

On the point of "making available", Mackenzie J did not believe that the individual to whom the material was made available needed to be identified, simply the fact that material was available to others needed to be proved.

Two additional points of note concern the discussion of strict liability and gain. Regarding strict liability, Mackenzie J considered that a defendant may raise absence of fault as a defence, but that if the actus reus was deliberate "the prosecution is not required to prove that it was the defendant's intention or purpose to make the publication available".[241] This appears contrary to the earlier jurisprudence (such as *Goodin*) where the courts were imputing knowledge or

[238] *Shaw v Department of Internal Affairs* [2005] DCR 989.
[239] At [8].
[240] At [4].
[241] At [14].

deliberateness as part of the actus reus in the context of possession. Mackenzie J also reasoned that the definition of gain could include "increased access" to other material within networks. He agreed with the judge of the lower court that gain is not only "monetary" and held that the appellant's participation wielded benefit that constituted gain. He further stated that no actual gain needed to be proved, or the quantum of expected gain.[242] It is unclear from the judge's reasoning why "gain" is included as an element of "making available" as the only particular offence that discusses it is s 123(1)(f).

Both these cases develop the law beyond the plain meaning of the statute in ways that both expand and collapse certain elements of the offences. With respect, this is an erroneous development of the law. Element (e) of Mackenzie J's five elements is not even set out in the offences of the FVPC Act. In the statute, "gain" is only described in subsection (f). It is one of the issues available for the court to examine but is not pertinent to subsections (a)-(e) and should not determine whether or not all the elements of the separate offences are satisfied. Both judgments lack reasoning on these points. The effect is to collapse the subsections of s 123(1) into a single offence and renders the distinctions between them defunct. This makes the earlier semantic wrangling over the distinctions seem superfluous and undermines the purpose behind Parliament distinguishing the offences in the first place. The distinguishing element of s 124 (i.e. knowledge that the publication is objectionable) should also merely tack on to the end of a finding under s 123(1), proved separately to the other elements of the offending. It certainly should not be integral to the finding under s 123(1) alone. Making the actus reus deliberate and intentional in the possession offence and unnecessary to the distribution offence is also confusing. This is despite the fact that it is almost impossible to imagine how a defendant could raise an absence of fault defence. Nevertheless, it is likely that the decisions are now precedent for future cases of s 123(1) offending (at least below Court of Appeal level). It is unclear what the implications are for ss 122(3) and 122(4). Principally, what is the purpose of the careful distinctions between providing access and facilitating access by transmission, if courts are so willing to ride roughshod over specific elements of particular offences?

In future cases, this precedent will further burden individuals, who cannot be sure as to what conduct amounts to certain offending, and also burden prosecutors, requiring them to prove additional elements not set out in the statute. This has implications for the right to freedom of expression. If an individual wishes to exercise their right, they can only do so knowing what the right does not extend to, that is, what is criminal. These offences should at least be clear

[242] At [11].

and certain so an individual can know how they apply. Uncertain as they have become, these offences unduly hamper individuals' ability to exercise their rights.

3 Liability under the FVPC Act

The advent of the Internet has thrown up the question of who can be liable for objectionable publications that are made and are made available on the Internet. To draw on the theories discussed above, a legal anomaly would occur if a party was able to avoid liability simply by conducting themselves online. There is no reason to presume that the FVPC Act cannot apply to parties online. A party operating online is still tied to the physical world. All Internet transactions can eventually be traced to a source and subsequent possessor. The Internet has not led to an "inalienable global commons": property rights prevail, tying assets to communications. A party (individual or corporation) that conducts themselves primarily online should not be presumed to be excluded from liability. An important point is that the FVPC Act is not only interested in individuals or end users. It was designed with companies that distribute expression in mind and this must extend to companies on the Internet. Yet no Internet company has ever been prosecuted under the FVPC Act. This does not accord with the fact that non-compliant publications are hosted on the Internet in New Zealand, having passed through many Internet companies to reach individuals' screens. In the end, it is users alone that find themselves bearing the burden of enforcement, which signals to the public that it is only individuals who can be made liable under the FVPC Act.

The biggest problem of liability under the FVPC Act arises less in identifying parties than in correctly applying the FVPC Act offences to the party most culpable. Historically, those who made publications widely available to the public were a concentrated group of industry players: this inherently limited the supply chain and it was simpler to attribute liability. Now this distribution model has changed to respond to the needs of Internet transactions. Internet users must use intermediaries' resources to create, store or send information. Information passes through these gatekeepers with varying degrees of knowledge, and thus culpability, as it travels from sender to receiver. This may amount to offending conduct by the user. However, if offending conduct is inherent to the way the technology functions, attaching liability solely to its end users seems unfair and outmoded. Further, if a user is not able to engage in the offending conduct without the service provided, does fault rest with the service provider for enabling such conduct? As an example, Reed highlights that because the transmission of packets takes place by copying, an intermediary can only operate by copying (potentially illegal) information; almost every intermediary that hosts third party content will have copyright infringing copies on its servers.[243] However, more than just providing the means to

[243] Reed, above n 75, at [4.2.1.1].

engage in conduct, these upstream parties can have a more immediate connection to the offending conduct. The problem is that, online, the structure and functions of such upstream parties often elude definition, allowing them to avoid liability. The status and liability of these parties is yet to be tested against the FVPC Act.

(i) The case of a tube site

In many cases, not only are upstream parties difficult to attribute liability to, but they are explicitly statutorily exempt from any criminal and civil liability resulting from expression carried on and coupled with their services. The FVPC Act appears to support the position that service providers are mere conduits or have no special interest in the expression their services carry short of providing access to that expression. Section 122 states that to distribute can mean to "provide access by means of a public data network to digital content", but does not include "to facilitate access to the publication by providing only some or all of the means necessary for transmission (other than by broadcasting) of the contents of the publication". An example of a person that does not distribute is "a network operator or service provider providing only a network or facility through which the contents of the publication are transmitted". This exception appears to exclude from distribution liability those that only provide users with access to their networks. However, a broader interpretation would also exempt any "service provider" who provides a service that allows distribution between users rather than directly from the service provider to the user. The distributor also must know of the act of distribution and what, in general terms the publication is or contains. Thus the section exempts any service provider that claims ignorance as to what publications are transmitted. This relies on disclosure by the service providers themselves of the extent of their monitoring capability. Importantly, the limitations of s 122 are that it only applies to the distribution offence, and does not necessarily generalise to the other offences of making, possessing and supplying.

Legal immunities such as s 122 are often the result of historic and successful industry advocacy (industry lobbying of copyright legislation being the plainest example of this in New Zealand). ISPs argue that they are "mere conduits" of information or "utilities" serving a public function. Additionally, they contend that they have no or very limited awareness of the information they are making available, prompting concerns about the fairness of attributing liability to them.[244] And finally they argue that liability would stifle creative and technological progress. However, there are weaknesses to such arguments, which presume that these companies are functionally equivalent to old telecommunications services. This inaccurately represents the true capability of intermediaries. For example, while the wiretapping of telephony services has been fiercely

[244] Uta Kohl *Jurisdiction and the Internet: Regulatory Competence over Online Activity* (Cambridge University Press, Cambridge, 2007) at 191.

debated in many jurisdictions, Internet companies have always monitored data stored on their servers (particularly in pursuit of commodifying that data). Not only are they not functionally equivalent to utilities but they have a vested commercial interest in the expression carried on their services.

A case study of one of these online companies sets out clearly the problem of attributing liability in the context of sweeping immunities in law. YouTube, for instance, describes itself as a "forum" and "distribution platform". Worldwide users are able to upload, store and curate video content through YouTube's services. YouTube also provide a paid subscription service *YouTube Red* which features original content produced in collaboration by YouTube. All the while, objectionable publications are available on the website and mobile applications and given the global penetration of the website, these publications are available in New Zealand. Putting the question of jurisdiction aside,[245] YouTube is unlikely to be made liable for making available objectionable content in New Zealand under the current legal framework. The first exercise would be classifying the type of offending they are undertaking and that would require defining their role in the Internet transaction. Timofeeva suggests that precise definition of those further upstream such as service and platform providers is "hardly conceivable due to the abundance of functions they perform".[246] Without knowing YouTube's specific technical capability it is difficult to determine what its role is in relation to the content made available on its service. Some things can be presumed: that data is hosted on their servers, that YouTube is able to remove data from its servers, and that this changes the rendering of data on users' displays. Anything beyond this is speculative. However, simply because a service provider is capable of monitoring data does not resolve the issue of knowledge. In the jurisdictions where liability can be attributed, "knowledge" and "reasonableness" often make it practically impossible to attribute liability without difficult-to-obtain evidence.

Given how the Internet is structured, such legal immunities remove incentives to monitor and/or act on expression hosted (even where such monitoring could prevent rights violations and other expression related harms). This immunity results in "permitting [private parties] to publish vast amounts of speech but not be held liable for that speech, while at the same time earning income through advertising based on personal profiling".[247] In other words, ISPs enable and profit from the existence of objectionable publications on the Internet, but have no

[245] YouTube is headquartered in the United States and is a registered company in Delaware. The extent of their legal presence in New Zealand is a "local version" of the site and the registration of the company domain name Youtube.co.nz and Youtube.nz.

[246] Timofeeva, above n 106, at 51.

[247] Anupam Chander and Uyen P Le "Free Speech" (2014) 100 Iowa L Rev 501 at 505.

legal obligations in respect of those publications. The victims of this paradox are the individuals who suffer from harm related to expression without legal recourse. Their only possible protection is their own investment in filtering mechanisms (or similar). All the while, they are still exploited for their data by these services and platforms.

The Law Commission once argued (in the context of defamation) that:[248]

> Whether a New Zealand ISP could be liable … would therefore depend on proving lack of knowledge without negligence. The standard of care in such circumstances would need to take into account the relevant standard practice of the industry together with any public policy issues such as whether or not a duty should be placed on ISPs to censor the material placed on their network by their clients, and if so, in what circumstances.

As standard industry practice changes so radically and with little clear policy position from this or past Governments, the Law Commission's proposal is not workable. Meanwhile, the only parties that can be targeted in this undefined legal area are end users, those using the services as intended by their providers but in such a way that amounts to offending conduct. The status quo gives private parties, such as YouTube, the benefit of the doubt, while necessarily offloading all liability to end users.

Not only are these parties able to escape any criminal liability under the current framework, but they also often seek to indemnify themselves against any private liability to individual users for the content they host. For instance, as part of its terms of service with users, YouTube claims an indemnity in respect of any loss caused by the relevant content:[249]

> You further understand and acknowledge that you may be exposed to Content that is inaccurate, offensive, indecent, or objectionable, and you agree to waive, and hereby do waive, any legal or equitable rights or remedies you have or may have against YouTube with respect thereto, and, to the extent permitted by applicable law, agree to indemnify and hold harmless YouTube, its owners, operators, affiliates, licensors, and licensees to the fullest extent allowed by law regarding all matters related to your use of the Service.

New Zealand case law reveals little about when a service provider will be liable for offending conduct. Most cases resolve in favour of the defendant service provider. No court has had the benefit of testing this under the FVPC Act. The most analogous examples arise from

[248] Law Commission *Computer Misuse* (R54, 1999) at 75.

[249] YouTube (accessed 12/10/15) <https://www.youtube.com/t/terms>.

defamation law. The Court in *Rafiq v Google New Zealand Ltd*[250] did not agree that the online service provider could be liable for defamation by providing hyperlinks to a defamatory blog. Doogue J, affirming the decision of *A v Google New Zealand Ltd*, suggested that the defendant (the service provider) did not have the "necessary connection with the publication of the material on the internet" to be found liable.[251] More recently, in the case of *Murray v Wishart,*[252] the Court of Appeal decided that the defendant (a social network page administrator) did not have actual knowledge of the defamatory content in question and thus they could not be liable for the defamatory act. By analogy, the decisions are consistent in principle with the exemption set out in s 122. If followed, a number of factual circumstances would be unlikely to incur FVPC Act liability: for example, providing access for "transmission" of objectionable content or providing a network/service where objectionable content is distributed, providing a platform featuring hyperlinks to objectionable content, or even featuring objectionable content itself (if the provider can demonstrate they had no knowledge of it). The effect is to immunise the majority of ISPs and other service providers from liability. Meanwhile publications remain available on these services until the users that deal with them are implicated. Even in advocating that ISPs should be exempted under the FVPC Act, Bayer points out that the mechanisms for attributing liability under the FVPC Act "do not help single out those perpetrators who may be harmful to society"[253] and the mechanisms appear unable to stem the influx of publications' available via service and platform providers.

4 New Zealand's case for jurisdiction on the a-territorial Internet

Lots of different activities have cross-border elements. The regulation of cross-border activity is resolved to a certain jurisdiction through different types of rules: legislation, soft law, and precedents that have emerged from conflict of laws disputes. The Internet has intensified the problem of whether the state purports to regulate the relevant conduct and whether it is right to do so. The FVPC Act is a New Zealand statute, applicable within the state of New Zealand. Like all statutes, there is a presumption against extraterritoriality. However, while tangible publications enter New Zealand borders through physical importation, online publications now enter New Zealand through a largely unfettered global network. This has undermined the jurisdiction of the FVPC Act, which was not designed with this distribution model in mind. A fundamental question is, is online conduct ever only territorial (occurring within the borders

[250] [2014] NZHC 551.

[251] At 19.

[252] [2014] NZCA 461, [2014] 3 NZLR 722.

[253] J Bayer *Liability of internet service providers for third party content* (Internet Society of New Zealand, Victoria University of Wellington Law Faculty, 2007) at 31.

of a single state) or is all online conduct now a-territorial and does this undermine the presumption against extraterritoriality? Clarification is necessary.

Generally, it is the case that online content laws disproportionally affect only some individuals and businesses. This is more problematic where those that are able to avoid complying are able to do so because they are domiciled overseas. New Zealand end users (i.e. those who consume the content), as opposed to foreign content distributors, are disproportionality affected by enforcement of the FVPC Act due to perceived jurisdictional limitations. Meanwhile those foreign content distributors, whose (potentially objectionable) content is accessible in New Zealand, are allowed to provide that content with impunity. Establishing whether or not the courts have jurisdiction over content that is accessible in New Zealand is an important step in adjusting this unequal burden in such a way that more fairly reflects the reality of who makes expression available. This is particularly pertinent for a country such as New Zealand, as the issue of jurisdiction affects most strongly "states which have fewer local online providers and which are more reliant on foreign content".[254]

The starting point of the FVPC Act is to determine if particular expression amounts to a publication. The publication must then be dealt with. The FVPC Act creates criminal offences which are subject to the Crimes Act 1961 which states, in s 6, that "no act done or omitted outside New Zealand is an offence". Section 7 of the Crimes Act does, however, provide for circumstances where there may be extraterritorial effect. Where any act or omission forming part of any offence, or any event necessary to the completion of offence occurs in New Zealand, it may be subject to New Zealand criminal law. The FVPC Act does not make provision for partially completed acts or omissions. However, in *Batty v Choven*, the Court dismissed the appellant's challenge to jurisdiction based on the fact that the appellant's primary distribution market for his offending activity was the United States rather than New Zealand. Speaking to s 7 of the Crimes Act 1961, Allan J said:[255]

> It is irrelevant that the appellant may have believed his primary market to lie elsewhere. It is likewise irrelevant that the server utilised by the appellant was situated in the USA. While in New Zealand, the appellant undertook certain steps to display or make available the images on his website. Those images were available to the respondent's inspector when he browsed the appellant's website from the inspector's computer in Wellington. There is therefore evidence that the relevant images on the appellant's website were in fact

[254] Kohl, above n 244, at 110.

[255] *Batty v Choven*, above n 215, at 27.

> displayed in New Zealand. All of the acts making up the actus reus are established and all occurred in New Zealand.

The case provides authority for the application of the FVPC Act to conduct which only occurs in part in New Zealand by a New Zealander. The case of *Department of Internal Affairs v Benning* also provides authority for the proposition that the offence does not have to be completed in New Zealand (a New Zealander distributing to an overseas person is subject to the offences of the FVPC Act).

In the case of a defendant (individual or distributor) sending or receiving publications while domiciled in New Zealand, the requirement for jurisdiction is plainly satisfied (even where publications are being sent to or received from a foreign state). If a foreign-based defendant is operating in New Zealand by way of a regional office or headquarters sending and receiving publications to New Zealanders, jurisdiction is also likely to be satisfied (although there may be issues regarding extradition). New Zealand courts do not have jurisdiction over foreign users in foreign states dealing with publications that originated in New Zealand. However, the question remains as to whether there is jurisdiction in the case of an overseas based defendant making publications available in New Zealand on New Zealand servers and devices. While many cases are tried in the absence of a defendant,[256] no court has ever tried an extraterritorial defendant under the FVPC Act.

New Zealand's historical experience with censorship informs this ambiguity of jurisdiction. Many publications have entered New Zealand from elsewhere. But in all respects, defendants have always been publishers, distributors, exhibitors and consumers within New Zealand. This is likely to remain the status quo, until some catalyst forces re-evaluation of this standard. If the majority of the publications reaching New Zealanders do not come from within New Zealand (as evidenced above) and are made available to New Zealanders by extraterritorial parties, this suggests that there is a significant gap in the law.

This is not to say that the FVPC Act does not contemplate any extraterritorial effect whatsoever. The sections that appear to set out extraterritorial effect explicitly are s 145A to 145C of the FVPC Act. The sections also appear to be exclusive, the FVPC Act only having extraterritorial effect in the context specified in the sections (that is, the extradition of those who commit certain offences relating to child pornography). However, the sections were plainly included in the statute in order for New Zealand to comply with its obligations under the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children,

[256] Criminal Procedure Act 2011, s 119–124.

Child Prostitution and Child Pornography. Unusually, the sections explicitly define "child pornography" in contradiction to the Department of Internal Affair's position of referring to such material as "child sexual abuse material". Furthermore, this definition is narrower than, and thus does not read synchronously with, s 3(2)(a) of the FVPC Act. The offending conduct stipulated by the amendments to s 145 is also narrower than the range of offences set out in the FVPC Act. It is arguable that the sections, the result of boiler plate drafting, should not be used to limit the substantive sections of the FVPC Act and are irrelevant when addressing the possible extraterritorial effect of the remainder of the FVPC Act. If anything, the section provides a model for how the entirety of the FVPC Act could apply to foreign defendants, if it were ever determined that a court had the jurisdiction to do so.

An argument against extraterritorial jurisdiction in the area of censorship law is the increased burden it would place upon online businesses (who would become subject to concurrent jurisdictions) and the economic implications flowing from this. Henn favours this view, suggesting that the website provider cannot choose which screens his content appears on and that they are dependent upon the surfer providing truthful identification information.[257] Given the advancement in identification technology, this claim should be viewed with scepticism. Henn did agree that where a website uses technology to target advertising to a specific user, they should be considered to have submitted to the jurisdiction of the specific user.[258] States can and do directly apply their laws to the Internet. Thus Kohl sensibly questions whether businesses have actually been discouraged from operating internationally under the threat of the resulting concurrent jurisdiction (or at least, that claims to that effect have been exaggerated).[259] This is particularly so because the lack of practical enforcement measures has prevented this hypothetical flood of extraterritorial proceedings. Kohl believes that arguments against a state asserting jurisdiction over the Internet because of futility or floodgates are "unappealing" and do not reflect reality.[260] States have looked to international law principles such as the protective principle and the passive personality principle for resolution.[261] There has also been much jurisprudential discussion on the principles of "minimum contacts" and

[257] Henn, above n 64, at 174.

[258] Henn, above n 64, at 175.

[259] Kohl, above n 244, at 104.

[260] Kohl, above n 244, at 73.

[261] See Yulia A Timofeeva "Worldwide Prescriptive Jurisdiction in Internet Content Controversies: A Comparative Analysis" (2004) 20 Conn J Int'l L 199; Niloufer Selvadurai "The Proper Basis for Exercising Jurisdiction in Internet Disputes: Strengthening State Boundaries or Moving towards Unification" (2012) 13 Pitt J Tech L & Pol'y; and Gillespie, above n 223.

"purposeful availment" with respect to websites targeting the destinations of their content otherwise known as "forum shopping".[262]

"Targeting" appears to be the favoured test for establishing jurisdiction. The test has its origins in American civil jurisprudence and was a way of establishing personal jurisdiction over Internet-using defendants. It has now extended to the realms of public and criminal law in many jurisdictions.[263] Mere presence on the Internet is generally considered to be insufficient to meet the test, but a certain level of interactivity and the nature of the information exchange are factors that will determine whether jurisdiction should be exercised. The principles of "country of destination" (where the content is made available) and "country of origin" (where the content originates) also assist in determining jurisdiction. Kohl suggests that a moderate targeting or country of destination approach is the most appropriate test for content regulation and one supported by courts around the world (which have rejected assertions that publishers do not know the location of those who access their sites).[264] The alternative, a country of origin approach, would almost always defer disputes to the jurisdiction of the United States or, as Kohl suggests, would lead to de facto harmonisation to the lowest common denominator.[265] The non-US consumer or victim would therefore have to bring or defend proceedings in a foreign place determined by reference to foreign law.[266] Henn recommends that there should be an international organisation set up to standardise the targeting test for non-civil disputes similar to the Hague Conference's Convention on Foreign Judgments in Civil and Commercial Matters.[267] Further, tests to determine whether a non-interactive website has targeted a specific jurisdiction should also be included in the resulting standard.[268] Targeting does come with limitations. While Timofeeva believes it is a reasonable and effective measure, she warns that the targeting test inherently lacks limiting principles.[269] To counter this, the United States adopts a reasonableness principle and Germany requires a reasonable link in their respective

[262] See Tracie E Wandell "Geolocation and Jurisdiction: From Purposeful Availment to Avoidance and Targeting on the Internet" (2011) 16 J Tech L & Pol'y 275; Kevin F King "Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies" (2011) 21 Alb LJ Sci & Tech 61; and Schultz, above n 62.

[263] Smith,

[264] Kohl, above n 244, at 150.

[265] Kohl, above n 244, at 184.

[266] Kohl, above n 244, at 181.

[267] Henn, above n 64, at 175.

[268] Henn, above n 64, at 175.

[269] Yulia A Timofeeva "Worldwide Prescriptive Jurisdiction in Internet Content Controversies: A Comparative Analysis" (2004) 20 Conn J Int'l L 199 at 211.

tests.[270] Furthermore, Maier believes that the UK's approach to online gambling requiring some physical link with the territory is even more rigorous, in showing deference to the impracticality inherent in regulating extraterritorial activity while also retaining control over sovereign territory.[271]

The absence of a jurisdictional test for the regulation of online publications by foreign defendants is a problematic gap in the law. For instance, as the FVPC Act has never been enforced against foreign defendants, this gives the impression that the country of origin approach is the test in New Zealand, although this is entirely supposition and inconsistent with New Zealand's civil law standard, discussed below. Kohl says that unfortunately for some jurisdictions (and unlike in other areas of the law) the law in this area lacks the benefit of principled decision-making in the finely textured context of actual cases.[272] Certainly, in New Zealand, the limited case law makes it difficult to identify any accepted approach. Drawing on private law by analogy is one way of bridging the gap. While there can be good policy reasons for derogating from consistency between civil and criminal law, it is inherently attractive that when a user goes online they should be able to anticipate their liability under civil, criminal and public law. This ability to anticipate liability would be greatly undermined if there are different jurisdictional tests for each area of the law. This might not be the case if there were strict jurisdictional demarcations on the Internet but there simply are not.

This is not to suggest that the issue of jurisdiction has been has not been addressed by the courts. Allan J said in *Batty v Choven*, obiter, that "[t]hose who use the internet, just like those who use the international press, have responsibilities as well as rights. The ability to reach internet viewers around the globe might well be accompanied by legal responsibility where the laws of other countries are infringed."[273] Smith provides a summary of the New Zealand position on cross-border Internet liability in civil law cases. Regarding defamation law, he highlights the leading case of *Obrien v Brown*[274] where the Judge decided that "there can be no question that publication on the Internet counts as publication for defamation purposes" and the case of *University of Newlands v Nationwide News Pty Ltd*[275] where the Court decided that, as the defamatory material could be downloaded in New Zealand, it could hear the

[270] Timofeeva, above n 269, at 205.

[271] Bernhard Maier "How Has the Law Attempted to Tackle the Borderless Nature of the Internet" (2010) 18 Int'l JL & Info Tech 142 at 169.

[272] Kohl, above n 244, at 48.

[273] *Batty v Choven*, above n 216, at [34].

[274] [2001] DCR 1065 (DC).

[275] (2004) 17 PRNZ 206.

dispute. Smith suggests that these rulings are consistent with the position taken by the High Court of Australia and English Court of Appeal.[276] In the case of trademark infringement, he suggests that New Zealand courts have similarly found that they will assume jurisdiction where the infringing use of trademark is directed at New Zealand computers and users, and where the New Zealand trademark owner may be harmed by the use.[277]

Judge David Harvey puts a spotlight on the civil case of *New Zealand Post Ltd v Leng*,[278] where the Court held that in order to establish jurisdiction in the case of defamatory Internet conduct three elements must be satisfied: (a) a website; (b) conduct that is purposefully directed at the forum state (New Zealand); and (c) knowledge that the plaintiff will be harmed in the forum State.[279] *New Zealand Post Ltd v Leng* plainly reflects the legal principles of a moderate targeting or country of destination approach: a defendant is liable based on the accessibility of the site in New Zealand. Harvey suggests that the underlying principles to such rules will need further refinement, particularly as the Internet grows and facilitates more Internet-based conduct.

Kohl also identifies that New Zealand takes a pseudocountry-of-destination approach with respect to online gambling.[280] The Gambling Act 2003 prevents foreign sites from being promoted, advertised or financed in New Zealand. This does not go so far as to criminalise sites operating in New Zealand, but does aim to minimise their effects and does not allow them to operate in a completely unregulated manner.[281]

It is suggested that, given the absence of clear authority in the criminal context, the more established precedent within civil law (a preference for targeting or country of destination) should be adopted in this area of the law as well. Harvey goes further and appears to suggest that there is scope in New Zealand's criminal law for a court to assume jurisdiction in the case of a foreign defendant conducting themselves online:[282]

> S 7 [of the Crimes Act 1961] provides New Zealand courts with flexibility for the recognition of initiatory as well as terminatory jurisdiction. Even where jurisdiction cannot be automatically inferred from the physical location of servers or the individual

[276] Graham JH Smith *Internet Law and Regulation* (4th ed, Sweet & Maxwell, London, 2007) at 629.
[277] Smith, above n 276, at 636.
[278] [1999] 3 NZLR 219 (HC).
[279] Harvey, above n 122, at 514.
[280] Kohl, above n 244, at 174.
[281] Kohl, above n 244, at 174.
[282] Harvey, above n 122, at 372.

> concerned, courts can assume jurisdiction, although a domestic connection is in fact required.

What implications would arise from the application of the FVPC Act to online publications, even in the case of a foreign defendant? A moderate targeting or country of destination approach would implicate the foreign content distributors who target the New Zealand jurisdiction through advertising or other means. The domestic connection may be founded on a range of evidence. For instance, if a New Zealander was specifically targeted by the foreign defendant or if New Zealand advertising appeared on the site, that would point towards a conclusion that there has been sufficient targetting to justify the exercise of jurisdiction. Accordingly, if the limited jurisprudence considered indicates anything, it is that it would be unreasonable to conclude there is no jurisprudential basis for the FVPC Act to apply to online publications that are (a) made available in New Zealand by foreign defendants who (b) target the New Zealand jurisdiction with their websites and (c) know that their websites have impact in New Zealand. Under this test, such defendants should theoretically be implicated in New Zealand's jurisdiction and answerable to its laws. If a foreign defendant was implicated in New Zealand law this would also throw up questions about the right to freedom of expression, whether it could or should extend to these foreign parties and whether and how limitation of their speech could be justified (unable to be explored in the space of this thesis).

Kohl believes that the issue of jurisdiction inevitably boils down to either making law more transnational or online activity less transnational, and that both strategies are being actively pursued by different countries.[283] This is because "there is no ideal solution which allows for freedom of online communication and the preservation of national laws at the same time".[284] Choosing which to compromise is based on value judgments and is unlikely to be resolved by legal doctrine.[285] For many jurisdictions, radically changing the law to respond to the slightest change in technological circumstances or "squeezing" old law into these new technological circumstances is inappropriate; incremental changes in laws is the better approach to tackling the issue.[286] Kohl suggests that any rules that do develop should be simpler rather than more complex and that increasingly meticulous fact-specific, case-by-case analysis undermines this goal.[287] While New Zealand lacks the legal and political clout to set international standards for how foreign online operators should be affected by jurisdiction, the jurisdiction has an

[283] Kohl, above n 244, at 28.

[284] Kohl, above n 244, at 254.

[285] Kohl, above n 244, at 289.

[286] Kohl, above n 244, at 45.

[287] Kohl, above n 244, at 85.

opportunity to adopt the legally preferred and internationally salient approach to jurisdiction: targeting. This may require a test case or legislative amendment. The issue of jurisdiction is not going away and its impact will only get more profound in the context of globalisation and increasingly Internet-enabled legal behaviour. The alternative of "doing nothing" will amount to ceding legal authority in this area to other jurisdictions or becoming a legal black-hole. Worse still, those with criminal intent might seize upon the regulatory gap in New Zealand, shaping New Zealand into the safe harbour illegal activity needs to flourish online.

It is worth briefly commenting on the limitations of practical enforcement, which continues to undermine many countries' assertions of jurisdiction. Even if a court states that it has authority to hear a dispute and make an order, there is no guarantee that the order will be followed by the defendant or enforced in the state where the defendant is domiciled. Clough summarises just some of the problems that arise in a public or criminal dispute with a foreign defendant:[288]

- Serious criminal offences are not often tried in absentia;
- Other countries are unlikely to enforce public law judgments therefore the defendant must be present in the prosecuting state;
- There may be competing claims for prosecution;
- Extradition is often underpinned by treaty and dual criminality requirements; and
- The relevant extradition treaty may adopt an enumerative rather than a prescriptive formulation.

Reed suggests that the alternative course to these burdensome procedures, extraterritorial enforcement action against a foreign defendant (such as seizing the foreign defendant's assets which are within the jurisdiction), "sends a clear message that the other state's laws are inferior, and thus less worthy of respect" and is more problematic legally and politically.[289] Few countries pursue this course successfully. The most well-known case of the ineffectiveness of enforcement is *UEJF et LICRA v Yahoo! Inc et Yahoo*.[290] The French Court, in this case, issued a public order against Yahoo for making available illegal Nazi memorabilia on its French site. Yahoo!, a United States-based organisation, did not comply with the order and sought to have the order declared unenforceable in the United States. The United States Court agreed stating that the United States may not enforce a foreign court order that chills

[288] Johnathan Clough "A world of difference: the Budapest Convention on Cybercrime and the challenges of harmonisation" (2014) 40 Monash University Law Review 698 at 707.

[289] Reed, above n 75, at 31.

[290] *UEJF & LICRA v Yahoo! Inc. & Yahoo!* Tribunal de grande instance [TGI] [ordinary court of original jurisdiction] Paris, 22 May 2000, (Fr).

First Amendment speech (a later appeal by the French was also unsuccessful).[291] The case serves to caution other states about sovereignty and comity. The enforcement jurisdiction issue more appropriately concerns the broader mechanics of international relations and cannot be addressed in this thesis.

5 Enforcing the FVPC Act online

The Internet's global distribution model that enables anonymous and interactive expression presents problems for censorship law. This is most pronounced in the area of enforcement. Historically, physical distribution sites (such as home video stores) could be inspected and physical publications could be seized, all before the expression therein could be widely disseminated to the public within the borders of New Zealand. For instance, the Unit recorded in 2000-01 that 403 video sites and 25 film sites were inspected (the Unit no longer records physical inspections).[292] The Internet has disrupted this enforcement strategy. No single response is sufficient to ensure compliance with censorship law. The Unit has been forced to prioritise: their greatest focus area is the sexual exploitation of children, to which the Unit takes a global view.[293] The current strategies used to effect this are: (a) running the web filter NetClean; (b) victim identification in objectionable images; and (c) national and international operations into the distribution and making of objectionable material including enforcing the FVPC Act in all aspects.[294] These will be elaborated upon below.

Enforcement has also been burdened by the fact that data on compliance is so difficult to obtain and measure. Where the Unit formerly reported outputs, they have since departed from this reporting model; the prevalence of Internet-based offending makes it difficult to measure outputs credibly.[295] For instance, there were 39 prosecutions of New Zealand offenders in the 2009-2010 period[296] and this dropped to 22 prosecutions in the 2010-2011 period.[297] Such figures do not account for other interventions the Unit makes, particularly with respect to teenage offenders, so comparison is of limited utility. The lack of compliance data produced by the Unit has contributed to the lack of data that quantitatively captures trends of public expression consumption and compliance with the classification scheme. There are no longer good measures of the effectiveness of censorship law and enforcement.

---

[291] *Yahoo! Inc v La Ligue Contre le Racisme et l'Antisemitisme (LICRA)* 169 F Supp 2d (ND Cal 2001) at 1192.

[292] Department of Internal Affairs *Annual Report* (2000) at 68.

[293] Interview with Steve O'Brien, above n 77.

[294] Above n 77.

[295] Above n 77.

[296] Above n 77.

[297] Above n 77.

The Unit's primary methodology with Internet offending is dubbed a "fly-fishing" approach, discussed in the short history section of this thesis. Like other enforcement agencies in this area, the challenge is capturing the most problematic offenders who can retreat to more secure online spaces (overlay networks such as the Dark Web are popular for now). The methodology glaringly reflects the uncertainty surrounding liability and jurisdiction, and the lack of alternatives available to the Unit when confronted with criminal expression being made available in New Zealand via the Internet by foreign parties. Ostensibly unable to make service providers and ISPs liable in any way for the expression being circulated, the Unit and other enforcement agencies must focus on the end points of the communication, that is, individuals (who may not be based in New Zealand).

The focuses of the Unit also inevitably exclude a large class of offending: compliance with restricted classifications. Section 23(2)(c)(i) of the FVPC Act, creates a class of classifications where a publication's availability is deemed objectionable unless restricted to a class of persons who have attained a certain age. These restricted classifications carry all the weight of the offending provisions under Part 8 of the FVPC Act and the according sentencing provisions. The OFLC reported in 2014 that 61% of publications submitted to the Office fell within this class.[298] Under the previous distribution model compliance with these provisions was much more achievable (the bottleneck of limited suppliers allowing for appropriate age verification measures). The Internet's distribution model coupled with user anonymity measures completely undermine this. Age verification protocols are easily overcome by the vast majority of users. The Unit does not have any overt policy on this issue. This has telling implications for the 61% of publications captured by the FVPC Act regime: (a) age-restrictions on publications are unenforceable on the Internet; (b) the only means of achieving public and industry compliance is presently voluntary compliance; and (c) to change this, a new compliance strategy is required for this class of publications. As enforcement is a vital part of the adequacy of the legal framework, the strategies used must be as effective as possible to meet the aims of the law. Measuring the effectiveness is a challenge but enforcement gaps such as this overtly undermine the entire framework.

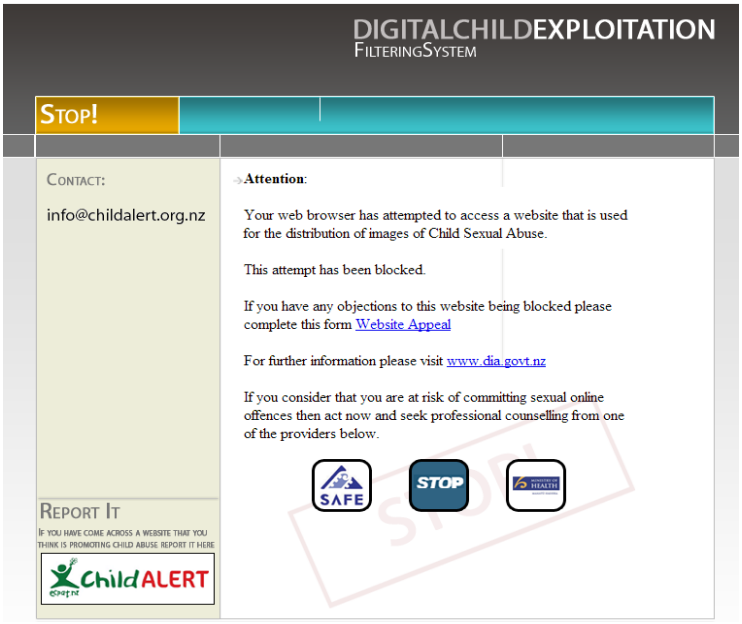
(i) NetClean

Trials for the web-filtering system, NetClean, commenced in 2008. A small group of ISPs agreed to trial it on their networks. Within two years the majority of ISPs in New Zealand had the filter operating on their networks through informal arrangements.[299] Although the FVPC Act makes a range of publications objectionable, the filter only applies to those websites that

[298] Office of Film and Literature Classification *Annual Report* (2014) at 13.

[299] Department of Internal Affairs *Annual Report* (2013-2014) at 14.

promote and support the sexual exploitation of children and typically only pre-pubescent children. This policy was developed to ensure cooperation from ISPs, along with the assurance that the filter would not be used as an enforcement tool. The Unit does not record, identify or monitor those who try to access sites displaying objectionable content. Further, a review process is built into the website. The following drop-down screen appears when the URL is requested:



To date the Unit has stressed that there has never been a legitimate appeal, although beyond the review mechanism facilitated by the Unit there are no legislative grounds for appealing the filtering of a website. There have been ministerial requests to review the material on the filter and, after a visit from the Ombudsman, satisfaction was expressed with the Unit's processes. The filter presently captures 100% of the mobile market and 90% of the broader market, preventing access to around 400-700 websites (although this fluctuates as sites are put up and brought down). At least one person monitors the filter 24hrs a day and the URLs for the websites are revised regularly. However, the Unit is attuned to the limitations of the mechanism, particularly as it only targets a limited application level aspect of the technology:[300]

> We stress that the filter is no silver bullet. A dedicated offender doesn't have to go to websites. They can use peer-2-peer. We can't filter peer-2-peer. There's also communication platforms.

[300] Interview with Steve O'Brien, above n 77.

All ISPs in New Zealand engage in some filtering of data, such as, spam, malware and viruses. The application of the NetClean filter to their systems simply requires applying another layer of filtering. As a result, members of the telecommunications and entertainment industry have also advocated for the NetClean filter to be expanded to include other content, such as that which violates copyright legislation. The filter has yet to extend to the other classes of objectionable expression. As the filter is not statutorily based, and depends on informal relations and voluntary compliance, any change to it occurs out of the purview of the public.

(ii) Relationship with the industry

Before the mass uptake of the Internet in New Zealand, the Unit dealt closely with the publication distribution industry, carrying out physical inspections of sites for objectionable material and labelling compliance. Even as late as 2007, 1600 inspections of the publication industry sites were undertaken.[301] Services providing content (entertainment and otherwise) online has meant that physical stores have now become all but obsolete, the number of physical inspections of sites declining in line with this change. As the distribution model has all but moved online, enforcement agencies are required to do the same. To date there has been no prosecution of a website operator in New Zealand making available content. Compliance is achieved through other means, including the industry's volition to be compliant. Sexually explicit websites in New Zealand, for instance, adopt protocols such as credit card verification and notification that the website contains adult content, to the Unit's provisional satisfaction. However, as already suggested, plenty of publications slip through the gaps. A large proportion of operators are not made to comply with the classification scheme via enforcement of the offence provisions (multi-nationals in particular). This may be due to the Unit not having confidence in their capacity to prosecute.

The relationship between the Unit and the online industry is largely informal, with no statutory basis for compelling disclosure from them if they believe objectionable expression is being made available as a result of their services or on their platforms. This informality requires negotiation and concession, as observed of the NetClean filter. One method of enforcement (used in other countries) is to execute search warrants on and then remove ISPs servers. New Zealand ISPs were assured this method would not be used by the Unit. However, the Unit can only go so far with its technical capability to determine the identity of offenders. Hence production orders are used to resolve IP addresses to physical locations. However, a production order can only be issued when the Unit can prove knowledge that the respective ISP has retained the information the Unit need. There is no legislation that requires ISPs to track or

[301] Department of Internal Affairs *Annual Report* (2007-2008) at 24.

retain customer data for compliance or to assist with the enforcement of the FVPC Act. There is also no consistent publicly available policy or industry standard for the retention of customer data. The Unit has to negotiate in good faith with ISPs in order to get the information they need. This is even more problematic in the mobile sector which increases a persons' connectedness to the Internet and has higher usage in New Zealand. In relation to overall industry compliance, Steve O'Brien suggests:

> To really operate we need to be stable in our own country. So we need high levels of voluntary compliance within the legal publication industry, so we need the government to start really developing a legislation around online content. To me they're trying for quick fixes when it's a really complicated issue that needs to be well, driven by industry. Its needs to be well thought through because it's changing so quickly.

Such comments reflect the fact that the law does not operate in a vacuum. Something more is required than informal cooperation and voluntary compliance if this particular law is to be adequately enforced.

(iii) International and inter-agency cooperation

The Unit favours a multi-agency approach nationally and internationally; this provides the flexibility which the Unit needs to overcome diplomatic obstacles while still maintaining its objective of a global approach to enforcement. Once New Zealand Police became involved in enforcement in 2008 with the OCEANZ team, the Unit worked closely with them to train them and improve their work. Other collaborations include Customs, the twelve respective Police districts as well as the Electronic Combined Law Agency Group and Netsafe via the Online Reporting Button. Maintaining these relationships requires ongoing management and diplomacy, given that they were founded through policy rather than statutory means. As discussed, the Unit's international cooperation strategy developed in the late 1990s under Interpol and at ECPAT's behest. Interpol pushed for unifying methods and tools including the use of filters. Thus New Zealand is involved in international liaison and training in a number of areas including technical development such as software for cracking new encryption methods and analysing data.

The Unit identifies that a mixture of informal and formal mechanisms is necessary to best effect international cooperation.[302] A range of individual contacts in various countries create a network that allows for intelligence information to travel relatively unfettered by

[302] Interview with Steve O'Brien, above n 77.

bureaucratic bottlenecks.[303] The United States Department of Homeland Security Immigration and Customs Enforcement team (ICE) have special agents based all around the world.[304] The Unit uses ICE's geographical reach to effect investigations based on the Unit's intelligence packages. Cultural barriers and the lack of technical capacity in some states can fetter cooperation, Russia, Japan and South Korea being examples. Formal measures are often more difficult to effect, but necessary in order to gain the necessary access to some enforcement agencies. While there is a memorandum of understanding with Australia, the Unit is attempting to develop one with the EU.[305] Liaising with Europol, for instance, requires going through a member state causing delay and sometimes uncertainty.

The Unit's global approach to enforcement, has led to multiple internationally coordinated operations. For instance, the Unit liaised with Interpol in 2011 to identify the top 50 offenders in the world. Intelligence packages were created and sent to enforcement agencies in the relevant jurisdictions. In New Zealand, a second tier offender was identified and a child rescued.[306] As discussed in the history section of this thesis, the Unit is able to participate in these operations because it construes Internet communications as public communications (unlike many other parts of the world). Their policy is derived from the rationale that if any member of the public could access the particular communication, then the communication is public. This policy has no statutory basis as the FPVC Act is silent on this issue. In the event that Internet communication was legally construed as private, the Unit's strategies (as they have come to be) would become impossible on the text of the FVPC Act.

The Unit's international cooperation strategy and attempts at procedural harmonisation are not reflected in the statute. That the statute does not address the global, a-territorial reach of the Internet or its technical particularities is evidently in contrast to the practice of the enforcement agency empowered to enforce it. This divergence becomes most problematic when the Unit's enforcement work is hindered because of the lack of clarity or sophistication of the statute or even more problematically if they are forced to act extra-judicially to meet their remit.

V A normative perspective on law on the Internet

This section argues that due to the challenges posed by the Internet and the inadequacies and weaknesses of the current legal framework, the FVPC Act now struggles to guide the behaviour of those it addresses. In other words, the statute's normativity has suffered. The

[303] Above n 77.

[304] ICE "What We Do" <http://www.ice.gov/overview>.

[305] Interview with Steve O'Brien, above n 77.

[306] Interview with Steve O'Brien, above n 77.

normative loss can be redressed with reform or seen as de facto evidence of the need for deregulation. But without the law to guide the choices of individuals on the Internet, technologists (who have no special or elevated competency when it comes to guiding/determining behaviour) will occupy this normative role, which will seed undemocratic and unethical outcomes for New Zealanders.

The FVPC Act aims to guide behaviour by addressing certain rules to individuals, namely, which expression is or is not objectionable in a free and democratic society. States regulate through legislation to serve some public interest goal which is unable to be met through private individual conduct or industry practice alone. In this case, the state is vested with a responsibility to protect children and other vulnerable groups, who are inequitably treated by the prevailing social and market conditions of unregulated speech. It does this by restricting the availability of particular publications. The law cannot fulfil these purposes if it does not have normative weight, that is, if it cannot or does not guide the behaviours of those it seeks to govern. Where individuals are not guided by nor comply with those rules, the normativity (and even legitimacy) of those rules is compromised.

There are a number of characteristics of normative law. Reed says that normative law on the Internet does the following:[307]

> (a) Identifies the behaviours which are likely to emerge from the innovation which is to be regulated;
> (b) Decides which behaviours are to be fostered and discouraged;
> (c) Devises mechanisms for persuading the human actors to behave in the desired manner; and finally
> (d) Resists the temptation to regulate the technology and not humans.

Further, it is not enough simply to enact laws, the law must entrench existing norms, clarify any uncertainties or ambiguities, or reinforce developing norms.[308] This is because, "[n]orms work from the perspective of the person who is potentially subject to the law, rather than from the perspective of the law-making state".[309] Finally, if (a) individuals do not understand the law as being addressed to them or (b) the law attempts to regulate a technology (or a method of acting) which has become outdated and is no longer in use, then individuals will not believe

[307] Chris Reed "How to Make Bad Law: Lessons from Cyberspace" (2010) 73 The Modern Law Review 903 at 929.

[308] Reed, above n 75, at 12.

[309] Reed, above n 75, at 18.

in the law's applicability.[310] Equally, the activity to which the rules refer must be a reasonably close match to the way in which the activities which it proposes to regulate are carried out in cyberspace.[311]

By way of example, Reed explains that the normative lapse of copyright law results from the impossibility for a user to make use of the Internet without copying and, because "copyright regulates the proxy of copying, not the use itself", users understand that this is not what the law aimed to achieve and do not believe that the law meaningfully applies to them.[312] Law that does not clearly set out the expectations of individuals to the benefit of their decision making is unlikely to result in compliance. Without compliance the law cannot be effective. Reed concludes: "A law-system which contains a high proportion of ineffective rules is, at best, in need of major improvement. A failure to achieve some minimum proportion of effective rules would seem to make it fair to describe the law-system as bad".[313] Brownsword goes further to say that this bad law is "wasteful", particularly where legislative or judicial resources are expended while maintaining the myopic view that "the regulatory position is as it was clearly intended to be".[314]

Normative law has a range of regulatory benefits. Yeung suggests that "most people are largely law-abiding and will effectively 'self-regulate' without the need for comprehensive and costly enforcement activity".[315] Thus, where law is normative and where it guides behaviour, compliance follows, reducing enforcement costs. Conversely, compliance with bad law is difficult to achieve and cannot be supplemented merely with heftier enforcement or broadening enforcement discretion. To best exercise their discretion, enforcement agents must know what the rules are and to whom they are addressed. Those trying to enforce bad law will only be able to guess as to how best to exercise their discretion to achieve the law's aims, if the position of the rule's addressees is unknown.[316]

---

[310] Reed, above n 75, at 13-15.

[311] Reed, above n 75, at 23-24.

[312] Reed, above n 75, at 155.

[313] Reed, above n 307, at 920.

[314] Roger Brownsword "So What Does the World Need Now? Reflections on Regulating Technologies" in Brownsword and Yeung (eds) *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing, Oregon, 2008) 23 at 27.

[315] Karen Yeung "Towards an Understanding of Regulation by Design" in Brownsword and Yeung (eds) *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing, Oregon, 2008) 79 at 93.

[316] Reed, above n 75, at 373.

The FVPC Act had been reasonably effective at guiding New Zealanders' behaviour and enjoyed a substantial degree of compliance, which was able to be measured. Now that the Internet is fully assimilated into daily life, there is little data that quantitatively captures the consumption of expression in New Zealand and public and industry compliance with the classification scheme. However, there is plenty of international evidence that young people (including young children) are accessing sexually explicit material online[317] and that users (regardless of age) are accessing illegal content, some because they do not understand what content is legal or illegal.[318] Anecdotal evidence in New Zealand suggests that this is the case here. The availability of publications has always been restricted to groups by age or other qualities (there are also those that are banned outright). Before the Internet, these rules were able to be enforced strictly because of the bottlenecks created by the distribution model, and to such a degree that the industry and individuals were at least aware of their legal responsibilities. Now, the rules are neither guiding behaviour nor being complied with. The most likely reason for this is that the Internet has changed New Zealanders' relationship with expression and the law has not responded to or evolved in response to this change. This loss of normativity has occurred gradually, corresponding with the increase of disruption caused by technological change. The weaknesses and inadequacies discussed above signpost where the language of the statute no longer matches the activities or addressees it proposes to regulate. Such anachronistic language has eroded the public and industries' ability to understand and meet the requirements of the FVPC Act and thus eroded the belief that the law applies to them at all.

Achieving normative law is a difficult balancing act. For instance, when does the law go beyond entrenching existing norms or reinforcing developing norms and begin to be autocratically deterministic of behaviour? Spinello persuasively argues that law which sets norms rather than the other way around may be laced with ethical problems for the addressee of the rule:[319]

> The law is not a panacea for solving market failures and imperfections. Frequently, individuals and corporations which depend too heavily on the law to guide their behavior are left floundering when there are "policy vacuums" or legal ambiguities. Following the law represents a legal externalization of moral judgment instead of its independent

[317] ATVOD "For Adults Only? Underage Access to Online Porn" <http://www.atvod.co.uk/uploads/files/For_Adults_Only_FINAL.pdf>.

[318] OFCOM "OCI Tracker Benchmark Study Q3 2012" <http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/online-copyright/Intro.pdf>.

[319] Richard A Spinello "Code and moral values in cyberspace" (2001) 3 Ethics and Information Technology 137 at 149.

> exercise. They must obviously be respected but this does not preclude making an independent moral assessment.

Where the law no longer appears to represent the legal externalisation of judgement, the law loses normativity. One view is that this signals that society is no longer dependent on the law to guide behaviour. There are a number of propositions that have to be accepted to adhere to this view in the context of Internet regulation:

a) That the law can be no more than a mere stopgap for unacceptable behaviour;
b) That individuals on the Internet, independent of the swaddle of law, act with reason and autonomy, ethically and in the interests of others; and
c) That technological systems (such as the Internet) and those that create them are morally neutral.

If this view is accepted, one generic solution is deregulation, to do away with the law, its familiarity and formalisation. However, Kohl suggests that the "substantial withdrawal of the State from the regulatory agenda … comes at a price: ultimate control over matters affecting their territory is in the hands of an outsider"; the approach "rejects legal diversity" and "would have drastic repercussions for large chunks of domestic law".[320] Spinello also does not appear to argue for abandonment of the law, he is merely critical of its heft in guiding individuals' behaviour.

Without state governance and legal frameworks, a vacuum is created, filled by other competing behaviour-guiding systems (such as economic models). Technology and technologists would be quick to assume the law's position. What is more, there are strong reasons to believe that technology is not merely biased to the preferences of its creators and therefore not morally neutral but that services and platforms are indeed autocratically determining users' behaviour. It follows that if there are ethical reasons for preventing the law from solely determining behaviour, there must be ethical reasons for preventing technology from solely determining behaviour. If legally immune, privately-owned, upstream parties are determining what the Internet experience means for New Zealanders, this experience is not likely to be a democratic one. As Kirby has observed:[321]

---

[320] Kohl, above n 244, at 270.

[321] Michael Kirby "New Frontier: Regulating Technology by Law and 'Code'" in Brownsword and Yeung (eds) Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes (Hart Publishing, Oregon, 2008) 367 at 381.

> … the fourth paradox is the coincidence, at the one time of history, of technologies that vastly enhance access to information… at the same time as they sometimes diminish genuine debate, enlarge unreviewable 'technological' corporate decisions and expand the capacity to 'manage' news in a way inimical to real transparency and accountability of decision-makers to the people.

Kim goes so far as to say, in aggregate, that the contracts that individuals must sign up to in order to access Internet services and platforms allow for service providers to obtain more rights while minimising their liabilities and increasingly resemble "unilaterally imposed private legislation, not as bargains".[322] Brownsword warns that while regulators are expected to operate in ways that are "transparent and accountable and that involve appropriate (inclusive) measures for stakeholder and public participation", technologists, conversely, have no special competency in values and choices and their opinions should be given no greater weight than the opinions of the public (citing David Bazelon).[323] One view is that technologists' strict adherence to rule sets will mean that the rules of the Internet will lack the reflexivity, nuance and discretion of the law. A more pessimistic view is that these technologists will inject their own biases into the technology (as they are entitled to do as owners of the infrastructure and services).

Technology also determines not just the acceptability of behaviour but whether that behaviour can ever actually occur. Hintz describes technologists as latent "policy makers" as the platforms and processes they create allow some actions and disallow others "…enables some uses and restricts others, and therefore occupies quasi-policy functions".[324] The issue of technology enabling and disabling behaviour has elevated the question of whether individuals can still exercise autonomy and choice if technology makes actions impossible (even the autonomous decision to break the law).[325] McIntyre and Scott use the case of technical filtering as an example of where moral accountability is not only shifted but reduced because users' choices are reduced and the reduced range of available actions signals to them "that those

[322] Nancy Kim "Internet giants as quasi-governmental actors and the limits of contractual consent" (2015) 80 Missouri Law Review 723 at 766.

[323] Roger Brownsword *Law and the technologies of the twenty-first century: text and materials* (Cambridge University Press, Cambridge, 2012) at 48-49.

[324] Arne Hintz "Outsourcing Surveillance - Privatising Policy: Communications Regulation by Commercial Intermediaries" (2014) 2 Birkbeck L Rev 349 at 354.

[325] Kenneth Einar Himma and Herman T Tavani "Regulating cyberspace: concepts and controversies" (2007) 25 Library Hi Tech 37 at 43.

actions which are not blocked are permissible".[326] While users may be morally intuitive about whether certain online expression is lawful, its unfiltered presence online and their ability to engage with it, must signal some permissive value. Moreover, users have no idea what expression they are being directed away from. Yeung believes that when technology effectively "designs out" people's choices, this risks denying them autonomy and that they then shift moral responsibility onto the system:[327]

> Such strategies risk inappropriately shifting moral and social responsibility for harmful criminal acts from the agents who commit them to the state who might be accused of failing to provide effective target-hardening solutions or, even more problematically, to victims themselves who fail adequately to protect themselves from criminal harm.

In the absence of state regulation, technology and the technologists are able to push responsibility for objectionable expression entirely onto individual users. They can claim that a "harm-free" Internet experience is a matter for the individual and what security services they can afford. Any risk is borne entirely by the individual. Without the law, a user (who historically has been protected from objectionable expression by the state and has been able to participate in the decision making process as to what amounts to objectionable expression through review and accountability mechanisms and electing representatives) now:

a) depends on service or platform providers to enforce breaches of their terms of use against offending parties or pay for additional security services themselves in order to use Internet services and platforms (with any luck) free from objectionable expression;
b) has no recourse or remedy available for being exposed to and harmed by objectionable expression made available by these service and platform providers; and
c) must defer to the non-transparent decision-making authority of Internet companies.

A system designed by technologists without the law does not in fact enable individuals to act autonomously. It reduces individuals' choices, is not democratic, does not foster responsibility and accountability and in no way mitigates the harms or inequities of speech. If the goal is that the Internet experience is one where individuals have the right to freedom of expression, including the freedom to seek, receive and impart information and opinions of any kind in any form and those who are inequitably treated by the prevailing social and market conditions of unregulated speech are protected, this system does not meet those goals. Instead, if this goal is

---

[326] McIntyre and others "Internet Filtering" in *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing, Oregon, 2008) 109, at 123.

[327] Yeung, above n 315, at 104.

to be realised, the law has to stand up and assert itself as a system of guiding behaviour on the Internet.

Because of disruptive technological change, the FVPC Act no longer matches the activities or addressees it proposes to regulate. This has eroded the public and industries' ability to meet the requirements of the FVPC Act and the belief that the law applies to them. However the alternative, deregulation, is not satisfactory. In lieu of legal frameworks, technology and technologists will undemocratically and unethically assume the role of determining behaviour on the Internet. Law reform is the better course.

The next question to ask is: what steps could be taken to address the inadequacies and weaknesses of the current legal framework, so that the FVPC Act might better apply to online expression and in a rights-consistent way. The rest of this thesis answers that question with a number of propositions. The reform proposed is inherently preliminary and only intended to be a starting point upon which further critique can build. Law change must account for:

- The law's purpose: what expression the FVPC Act aims to address, what can be done with that expression and to whom the rules apply;
- Whether the Internet is viewed as a public sphere or alternatively as just another communication medium. An approach must be adopted and the law must accord with the chosen approach. The latter approach is the correct one.
- The guidance given by the courts as to how the classification scheme is or is not consistent with the right to freedom of expression.

The task of returning to principled normative language in the statute is a relatively simple one and one that should be taken up by lawmakers interested in the FVPC Act being an adequate legal framework to regulate online expression.

A Making a choice: the Internet—private marketplace or public sphere?

Before addressing the proposed reforms, a particular principle of Internet regulation must be dealt with. That is, whether the Internet is a public sphere, a characteristic which would elevate it above other telecommunication technologies. The discussion of this principle leads into why the reforms proposed were chosen. If the Internet is a public sphere, it cannot be treated in a functionally equivalent way, new rule-sets/laws need to be created to regulate it and those that provide access to it (and services and platforms on it) may be deserving of special treatment or exemption by the law. Thus either (a) the Internet is just another communication medium like print or broadcasting and the new features of the medium, such as global reach, enable unheralded expressive acts that existing law can regulate or (b) the Internet is more

transformative than any of its technological predecessors and that it is a public space that serves a public function. Much has been written on the latter approach[328] (an adaptation of Jürgen Habermas' theory of the public sphere), particularly since Johnson and Post's seminal thesis on the Internet as a "new realm", able to subvert traditional territories and set its own norms and laws.[329] Many scholars subscribe to this view.[330] The argument suggests that because the Internet (a) allows for deliberative discourse, (b) has potential for community building and (c) enables an unrivaled breadth of connectivity, this means that it at least represents something public, if not a truly public sphere. Himma and Tavini argue that "if the Internet is viewed as a public space, then there are good legal and moral reasons for ensuring that everyone has access to it", however if the Internet "is viewed as a medium of some sort, then an entirely different set of rules apply".[331] Arguably the problems with Internet regulation in part persist because states do not adopt an approach and then do not regulate accordingly and consistently.

The contrary view, and the position taken in this thesis, is that the Internet has not become a public sphere and should therefore be treated as a communication technology, inhabited by private actors. While Laidlaw adheres to the view that the Internet is constitutive of "multiple spaces, some public, some private, with multiple public spheres", she highlights that Habermas himself actually rejects the proposition that the web can produce a public sphere.[332] This is because, while the Internet may have been created under the auspices of being a public sphere (reflecting Habermasian ideals) the Internet is or is likely to become entirely commercialised, mirroring the experience of its communication predecessors. There is little to suggest that the

---

[328] See JR Reidenberg "Lex informatica: The formulation of information policy rules through technology" (1998) 76 Tex L Rev 3 553; Lawrence Lessig "The Law of the Horse: What Cyberlaw Might Teach" (1999) 113 Harvard Law Review 2 501; JL Goldsmith and T Wu *Who controls the Internet?: illusions of a borderless world* (Oxford University Press, New York, 2006); and Joshua AT Fairfield "Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life" (2012) 27 Berkeley Tech LJ 55.

[329] David R Johnson and David Post "Law and Borders: The Rise of Law in Cyberspace" (1996) 48 Stanford Law Review 1367 at 1367.

[330] See M Poster "Cyberdemocracy: Internet and the public sphere" [1997] Internet culture 201-218; L Dahlberg "The Internet and democratic discourse: Exploring the prospects of online deliberative forums extending the public sphere" (2001) 4(4) Information, Communication & Society 615-633; Z Papacharissi "The virtual sphere: The internet as a public sphere" (2002) 4(1) New Media & Society 9-27; Diana Saco *Cybering democracy: Public space and the Internet* (Vol 7, University of Minnesota Press, 2002); and Jürgen Gerhards and Mike S Schäfer "Is the internet a better public sphere? Comparing old and new media in the US and Germany" (2010) 12(1) New Media & Society.

[331] Einar Himma and Tavani, above n 325, at 39.

[332] Emily B Laidlaw *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility* (Cambridge University Press, Cambridge, 2015) at 16.

Internet creates a space that is truly democratising or enables the conditions that realise free speech any more than any other communication medium.

Firstly, the conduct of service providers negates the presumption that the Internet is a public sphere. Private companies own and control most of the Internet's infrastructure and have not relinquished their property rights and profits in favour of a global commons. Shackelford believes that privatising cyberspace with property rights is likely to turn it into another medium like television, and the Internet would simply mimic the evolution of the telecommunications sector, with incumbents eventually dominating the medium.[333] Also, the disparate self-regulatory codes of Internet companies are "insufficient to the task of facilitating the internet's democratic potential".[334] These service providers are also typically quick to assert that they are parties in private transactions with their customers (see YouTube's terms of use as an example). The trending "Freemium" online business model also has little democratic ambition and actually undermines individuals' speech rights.[335] Short of actual payment for their services, these companies and their shareholders are primarily concerned with the ability to harvest data and then profile individuals as consumers (filtering in and out relevant content to maximize the potential for viewership to be converted into profit), not truth, democracy or self-expression. Lambers predicts that this filtering of data on the Internet will lead to the "sovereignty of consumer choice", that is, the "marketplace of ideas truly becoming a market".[336] If this prediction is realised then the Internet looks a lot more like a private space where merely connecting to the Internet is a transaction and less like a public space for expressive acts.

Secondly, there are increasingly examples of states attempting to rebut the idea that there is no public interest in the Internet by actively constituting the Internet as public. France and Costa Rica have both constitutionally declared access to the Internet is a human right. In the United States, ISPs had engaged in blocking, throttling and other means of controlling users' access to the Internet and content in non-transparent and discriminatory ways. When the Federal Communications Commission (FCC) tried to order Comcast to stop throttling peer-to-peer traffic, the US Appeals Court declared that the public agency had no authority to do so as these

[333] Scott J Shackelford "Toward Cyberpeace: Managing Cyberattacks Through Polycentric Governance" (2013) 62 American University Law Review 1273 at 1315.

[334] Laidlaw, above n 330, at 233.

[335] See comments by Chris Hoofnagle "Free: Accounting for the Costs of the Internet's Most Popular Price" (2014) 61 UCLA L Rev 606 at 669: "While free has become the default price for Internet services, consumers are made vulnerable by the hidden costs: the monetization of their personal information and in such a way that exempts them from qualification under consumer protection and privacy laws".

[336] Lambers, above n 68, at 106.

companies lacked "any statutorily mandated responsibility".[337] It was not until 2014, after a subsequent Federal Appeals Court ruling, that the FCC decided to classify ISPs as "common carriers" bringing them within the FCC's remit.[338] The state agency had to declare that there was a public interest in the practice of ISPs to make these private companies subject to any public mandate. There does not appear to be strong political volition in New Zealand to similarly constitute the Internet as a public space in a similar way or otherwise regulate the markets enabled by the Internet, particularly not in the public interest. The little regulatory action that has been undertaken has been in the competitive interests of New Zealand businesses.[339] Significantly, there is no New Zealand legislation that deals with ISP behaviour in relation to discriminatory practices that undermine individuals' access to the Internet and fetter online expression. As highlighted in InternetNZ's discussion paper on this issue there are real concerns, "about the power of ISPs to control access to information distributed over their networks for their sole commercial gain".[340] If private companies determine whether or not an individual can access a space, and then how they can access and use that space, then it is specious to suggest that the space is truly public.

The fact is, New Zealand lawmakers have improperly relied on this public sphere approach, and in such a way that elevates the status of the Internet and Internet companies to such an extent that they have become impervious to law and enforcement. Not only is this to the detriment of the law and its aims but it puts individuals at a disadvantage. Even in a context where the law regards the Internet as public, individuals not only have to pay to access the Internet and Internet platforms and services (which creates barriers to the exercise of speech rights) but have to contract security services to prevent crime or other harm to themselves. They then are unlikely to have legal recourse against those platform and service providers that host the harmful content or breach their contractual right to access or limit their expressive rights. In practical terms, this is antithetical to all ethical and legal understandings of a public sphere and the role the state should play in it.

---

[337] *Comcast v Federal Communications Commission* 600 F 3d 642 (DC Cir 2010).

[338] The White House "Net Neutrality" <https://www.whitehouse.gov/net-neutrality>.

[339] For instance, the New Zealand government's plans to have consumers pay goods and services tax on their online purchases. This was supported by New Zealand businesses who claimed that the regulatory gap led to an unfair playing field, while it was eschewed by others who claimed unjustified interference. See Todd Mclay "Tax bill tackles offshore property speculators and online GST" (press release, 8 December 2015) and Chris Keall "Tax reform: govt should go further and target multinationals' profit-shifting – Spark boss" *The National Business Review* (online ed, New Zealand, 19 August 2015).

[340] Internet NZ "Net Neutrality" (June 2015) <https://internetnz.nz/content/network-neutrality-discussion-document>.

VI A rights-consistent vision of New Zealand's censorship strategy

This thesis has dealt with the many legal challenges posed by the Internet. It has specifically addressed the weaknesses and inadequacies of the FVPC Act. This final section proposes a way forward: modernisation of the law that better distributes the burden of harm and aspires to be rights consistent.

As discussed, the courts have not declared that the classification scheme set out in the FVPC Act is inconsistent with the right to freedom of expression which would signal to Parliament the need for revision. The reading down of the terms in the FVPC Act may have changed the approach taken by the classification bodies, but not the scheme envisioned by the FVPC Act itself. The Supreme Court in *Spark*, in particular, seemed to consider that the right does not extend to or protect objectionable publications. The logic is somewhat circular: the limitation of expression by the state is demonstrably justifiable if done in a demonstrably justifiable way. In lieu of judicial comment to the contrary, the conclusion must be that the FVPC Act is demonstrably justifiable. Ideally, New Zealanders should know what is and is not protected expression based on this legal framework. However, without more precise rights commentary and in the broader context: one of much recent technological, economic and socio-political change, other norms (such as technologically-enabled online expression signalling permissive value) have been promoted and now shape New Zealanders' choices in relation to their expression online.

Another theme that has emerged from this thesis is that because the law no longer reflects the experience of Internet users (meaning it is not understandable and regarded as applicable to them), the law's normativity has suffered. The law needs to be modernised in order to recoup its normative weight and be fit for purpose, that is, to regulate online expression adequately. Those sections that appear most wanting include the definition of the term publication and the offence provisions.

In light of this, this thesis recommends three proposals for reform:

- First, address the language of the statute so that it can be clear, rights consistent and futureproof.
- Secondly, re-evaluate the rights-consistency and normative value of filtering, or technological fixes, as one of the primary mechanisms for stopping the availability of objectionable publications in New Zealand.
- Thirdly, revise the role that those who provide Internet services and platforms have in restricting the availability of objectionable publications in New Zealand, with a view to doing away with any legally based exceptions that immunise them from all liability.

There are many other aspects of the FVPC Act that are worthy of scrutiny (which it is not possible to cover in this thesis), but these proposals are the least that could be done to address the normative lapse.

A Amending the language of the FVPC Act so it might better apply to online expression

Re-defining publication

The definitional problems with "publication" need to be addressed first if it is to adequately apply to Internet expression. If defining publication was ancillary to the purpose of the FVPC Act, the current expansive and highly appended definition would not be so problematic. However, it is the availability of the "publications" themselves that the FVPC Act presumes causes harm and this is the entry point upon which the classification bodies engage in their statutory duties.

Any change to the definition must take account of the conclusions of the FVPC Act rights jurisprudence, as change could upset the fine balance achieved between the classification scheme and the right. What amounts to a publication was one of the issues in the Court of Appeal decision in *Spark*. Not only was it decided that the definition of publication was entirely separate from the issue of availability ("it contains no requirement of availability, nor does it even hint at such a requirement")[341] but it was also insinuated on appeal that once the Classification Office has decided that a publication is objectionable, the expression contained therein was never protected expression. It follows that the right to freedom of expression is not limited by the application of the FVPC Act to objectionable publications. This applies to the host of objectionable publications already classified by the Classification Office and the future ones yet to be classified. It is within this context (where the scope of the right has been deflated by the courts) that a clear understanding of what a publication is, is necessary to ensure that the right is not further limited. This enables individuals to assert their right against the state effectively if and when an unjustifiable limitation does take place.

The New Zealand lay person is unlikely to be able to articulate what a publication is on the Internet and therefore how the FVPC Act applies to their Internet use. This is in part because the statute covers not only commodified (commercial) expression, distributed to the public by industry in a linear fashion (e.g. films streamed on online platforms), but also non-commercial expression possessed and distributed between private individuals (e.g. messages exchanged on messaging apps). In the contest between individuals' rights and the rights-limiting actions of the state, not being able to determine what a publication is amounts to a handicap for citizens.

[341] *R v Spark* [2009] NZCA 345, [2009] 3 NZLR 625 at [25].

Uncertainty has meant that it is essentially classification bodies that decide what a publication is. This uncertainty has negative implications for the normative effect of the law and also the rights of individuals.

Questions hang over what constitutes a publication and ideological hurdles prevent wider application of the FVPC Act (the classic bulwark is that the definition of publication cannot apply to digital media, even if this view has been largely overruled by the appendages to the legislative definition and the practice of the classification bodies). If the FVPC Act is to overcome such hurdles, this requires a plain, clear and certain definition of what constitutes a publication. The current definition is in practice applied successfully to a number of online publications, particularly objectionable ones. However, its wider application is hindered by the restrictive and outmoded use of terms (at a minimum “films” and “videos”) and inaccurate interpretation, rooted in technological determinism.

The revision of the definition should aspire to be technologically neutral (i.e. it must resist regulating technology rather than the behaviour it seeks to deter). The definition should reflect the way in which publications are made available. At a minimum it must be capable of being discoverable and capable of being submitted to the Classification Office. An amendment to the definition should also take the opportunity to return to and make a statement about the law’s purpose. It is the availability of the harmful expression in publications that the law aims to regulate. This purpose should not be frustrated because of the technical platform or means used to make that expression available, particularly as the expression is held to be injurious to the public good irrespective of the platform. Finally, this definition should not unduly limit the right to freedom of expression. The position taken in this thesis is that such a definition would be capable of being applied to online expression.

Compare, for instance, the definition of a publication to that of a “digital communication” as defined in the s 4 of the Harmful Digital Communications Act 2015. The definition provides that digital communication: (a) means any form of electronic communication; and (b) includes any text message, writing, photograph, picture, recording, or other matter that is communicated electronically. This definition plainly suggests significant cross-over between publications and digital communications. And yet the later definition is more succinct, clear and intelligible than the former, easily translating to the user’s online experience. The digital communication definition certainly captures a wide range of expression (wider still than the FVPC Act), but does not do so in a way that uses inscrutable terms such as “thing” (found in s 2(d) of the FVPC Act). While there may be policy reasons to maintain some distinctions (such as that

between broadcasting and the FVPC Act), there are few for maintaining the current definition of publication as it stands in the FVPC Act.

Revising the language of the statute does not have to be an imaginative exercise. Rather, it could be as simple as removing the excess from the current definition. An alternative definition of publication may be, "any text, imagery (moving or still) and/or sound recording". This definition is clear, addresses the needs of prior restraint, and is not tied to a particular technology. All of the current examples of publications within the current definition are folded within this alternative definition minus the technologically deterministic language and confusing conjunctives. The omission of the word "electronic" is also deliberate for this reason. The definitions of film, video recording, book, etcetera, in s 2 of the FVPC Act also become superfluous on this alternative definition. References to these within the wider statute could be replaced with the catch-all term "publication". This definition meets all the requirements set out in the preceding paragraphs and does so while being worded in a way that is clear and intelligible to those it intends to address: the public and industry. The definition is also progressive in that it can apply to old media (film and literature), new media (Internet expression) and whatever the future has in store.

Issue may be taken with the fact that the definition still covers non-communicative expression but this has been laboured over by other authors and is not capable of being addressed within the scope of this thesis.[342] Additionally, any amendment to the term publication will not affect the subject matter gateway provision. This provision imposes an immediate limitation on the reach of the censorship laws. Expression that does not deal with the matters specified in s 3 of the FVPC Act will not be captured. The change of language anticipates and is flexible to inevitable change in media by which New Zealanders express themselves. While more expression may be examined this better fulfils the aims of the statute and does not mean expression will be unjustifiably limited.

Re-defining the offences of the FVPC Act

The s 123 offences of the FVPC Act also no longer reflect the reality of how users receive and engage with publications. The demarcations between copy, supply, distribute, import, displays or exhibits have been rendered all but obsolete online. None of these terms, in lay or legal meaning, practically reflect how publications are made available on the Internet. Supply and distribute have been convoluted by their qualifications and exceptions elsewhere in the statute. These offences have also not been applied consistently to the same online activity, particularly

[342] See, for instance, the critique of possession in Dean Knight, above n 206.

the storage and transfer of files between hardware devices. There is some irony in the fact that the harm (that is the basis of its criminal severity) is in making a publication available, yet this language cannot be found anywhere in the offence provisions. Gillespie highlights "making available" is the term used in the majority of Australian states' obscenity statutes.[343] "Publish" is the term used in the Obscene Publications Act 1959 (UK). US Child Pornography offences simply use the terms "distribution" and "reception". In this slew of terminology, Gillepsie calls for a "rationalization" of the law, as does Clough:[344]

> …"making available" can include an inchoate element in that it should not be necessary to prove that distribution has happened but it will include situations where the police can prove that it is possible to gain access to the images stored.

The New Zealand courts have engaged in creative statutory interpretation and gone some of the way to compact these separate offences into a single comprehensible offence. It is argued that despite the best intentions, this creative interpretation has made the law unclear. For instance, when an individual streams video from a foreign source, it is disingenuous to suggest that they should recognize that they are importing a publication, particularly if there is nothing to earmark this on the website or application they are using. That the provisions have been incorrectly applied to fact scenarios by the courts is likely to be because of the inflexibility of the tightly defined bands of offending, based on analogy to pre-Internet means (predominantly ones like cinemas, bookstores and post). These provisions must be revised for the sake of certainty, particularly so that they can be easily understood by the industry and individuals they intend to address, accurately reflecting the way that Internet transactions work and are experienced by the user online. Again, the law must regulate the behaviour and resist regulating the technology and/or avoid being tied to a particular technology. To do so it must be as plain and neutral in its use of terms as possible. If the law seeks to punish those who make and send and receive objectionable publications then it should say just that.

A "making available" offence (instead of the listed offences under s 123) would not be technologically deterministic in the way "copying" or "importing" is. There may be a policy interest in determining that making available for "gain" is considered an additional aggravating factor akin to the knowledge that the publication is objectionable, but there is no reason for the law to perpetuate artificial boundaries between the offence provisions to the extent that they no longer reflect the reality of online communication. The tiers of offending would be truncated to possession, making, and making available.

---

[343] Gillespie, above n 221, at 207.

[344] Clough, above n 288, at 351.

Of course it is not suggested that changes such as these are the panacea needed for the statute. This exercise merely aims to highlight the simplicity of revising the key tenets of the statute in a normative and rights consistent way likely to withstand future hurdles, be they technological, ideological or otherwise.

B The fallibility of filtering: is a filter the best means of upstream regulation?

The adequacy of a legal framework that seeks to apply to online expression depends not just on the text of legislation and its interpretation but on the feasibility of its application and enforcement. This thesis now turns to the role that enforcement plays in the law's normativity. A legal framework is "bad", as Brownsword suggests, where enforcement resources are being directed and expended only on targets at the extreme end of the spectrum, excluding large classes of offending and culpable parties from enforcement. A law that limits the expressive rights of some while excluding others, the only justification of which is allocation of enforcement resources, does not sit well with the sentiment of NZBORA. Moreover, the notable absence of enforcement on the Internet also signals a permissiveness of objectionable expression undermining the law's aims (which is amplified in a context where the language of the statute does not direct individuals to self-regulate). Current efforts of upstream enforcement such as filtering are not sufficient, yet it is their persistence that may hamper the development and future of censorship law and enforcement.

Of all the censorship tools available to regulators, filtering is one of the most contested. Yet filtering is a significant feature of New Zealand's enforcement strategy. The technical development in this area means that the precision of these filters is unpredictable. NetClean can filter down to the contents of the image but typically the URL itself is blocked, not just the image on screen. Other types of filters include:[345]

> … discriminatory ISP licenses, content filtering based on keywords, redirection of users to proxy servers, rerouting packets destined for a specific IP address to a blacklist, website blocking of a list of IP addresses, tapping and surveillance, chat room monitoring, discriminatory or prohibitive pricing policies, hardware and software manipulation, hacking into opposition websites and spreading viruses, denial-of-service (DOS) attacks that overload servers or network connections using ‘‘bot herders,’’ temporary just-in-time blocking at moments when political information is critical, such as elections, and harassment of bloggers (e.g., via libel laws or invoking national security).

[345] Barney Warf "Geographies of global Internet censorship" (2011) 76 GeoJournal 1 at 3.

Filtering is plagued with legality and legitimacy concerns. As put by McIntyre and Scott:[346]

> Much of the policy making and implementation in respect of Internet filtering occurs through other mechanisms involving different actors with risks both to the transparency and accountability dimensions which, through conceptions of the rule of law, underpin legitimacy in governance.

In the UK, the Internet Watch Foundation has repeatedly had to defend itself over claims of over-blocking, with a number of instances of inaccurate consignment of legitimate sites to its blacklist. Villeneuve also says there is growing evidence that "filtering is perceived as cooperation, thus conceptually negating the need to engage in dynamic cooperation".[347] While filtering has all the pretence of part of a wider co-regulatory strategy, it is often where the buck stops in terms of government and industry working together to prevent harm. As Villeneuve goes on to argue: "Not only do the domestic organizations charged with compiling lists of offending child porn … lack the willingness or ability to reach out to relevant non-state actors across national boundaries, but they also have reduced incentive to do so."[348] A lackadaisical attitude can develop in regulators who believe that their population is entirely "protected" because filters are in place. It also removes the onus on private actors to engage in any prevention, identification and enforcement mechanisms.

The Unit regard NetClean as simply one of its tools in the tool-kit but this does not resolve legitimacy concerns. The filter is not endorsed by legislation, is not reviewable and relies on the cooperation of New Zealand ISPs to be effective. If all New Zealand ISPs decided tomorrow to remove the filter, there is no statutory authority to stop them. One of the concessions made to maintain this cooperation is that the only material filtered from the New Zealand public is extreme child abuse material. All other objectionable material is accessible to New Zealand Internet users. New Zealanders may already regard the context of online expression as different to expression in the physical world. The absence of a broader filter that blocks all objectionable publications may signal to New Zealanders that what remains is acceptable expression, promoted by the platforms they use, and tolerated by the state.

The filter's basis in voluntary compliance by ISPs also limits its effectiveness and exposes the classification scheme to criticism (particularly as to whether it is a justified limitation on the

---

[346] McIntyre and others, above n 326 at 115.

[347] Nart Villeneuve "Barriers to Cooperation" in Deibert and others (eds) *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace* (MIT Press, Cambridge (Mass), 2010) at 63.

[348] At 66.

right to freedom of expression). Although a product of its cultural context, the example of the United Kingdom's experience with filtering should act as a warning to New Zealand. Having a charity decide what is objectionable and then forcing ISPs to put in place a filter based on those decisions is "to surrender judgments about what comprises the public interest to private and unaccountable groups [and this] may be seen as a dangerous development that needs to be curtailed if the freedom of online expression is to be effectively safe-guarded".[349] Nair and Griffin argue that the use of filters, opt-in access to the Internet, ISPs and non-government regulators being co-opted into state regulation, and the rise of surveillance has paved the way for a new regulation design intended to replicate Bentham's Panopticon and, as a result, the individual can never know whether he or she is being observed or know what is permitted content and what is not.[350] They believe that if the aim of the law is to provide a framework through which dissemination of expression may occur but still place limits upon it, the state needs to cease to focus on the end user and refocus its attention back to the distributor, giving individuals the confidence to enjoy a degree of communication with the State in terms of what should, and should not, be regulated.[351] These criticisms have resonance with the New Zealand experience, particularly given the enforcement focus on end users and the introduction of the mere viewing offence which will only increase scrutiny on end users.

The extra-legal nature of the strategy is also a red flag in terms of the right to freedom of expression. Is the filtering of objectionable publications on the Internet consistent with the right to freedom of expression? Historically, physical sites were inspected by enforcement agents who seized objectionable publications in New Zealand or at the border, before they could be further disseminated to the public. The prior restraint activity of filtering appears no more onerous than this historical practice, which enjoyed a high level of acceptance by the New Zealand public. This practice is also supported by a conservative reading of the rights jurisprudence: that there is not a right to seek, receive, and impart objectionable publications on the Internet. On this simplistic view, the filtering of (at least) objectionable publications is likely to be regarded as justified and this is the view which is adopted by the Department of Internal Affairs.[352] That said, one of the requirements of NZBORA is that a limitation is only justified if it is "prescribed by law".[353] The intention of this requirement is to "preclude

[349] Jewkes, above n 101, at 551.

[350] Abhilash Nair and James Griffin "The regulation of online extreme pornography: purposive teleology (in) action" (2013) 21 International Journal of Law and Information Technology 329 at 348.

[351] Nair and Griffin, above n 350, at 352-353.

[352] Department of Internal Affairs "Common Questions and Answers" <https://www.dia.govt.nz/Censorship-DCEFS-Common-Questions#6>.

[353] NZBORA, s 5.

arbitrary and discriminatory action by government officials".[354] A rights infringing action not prescribed by law still amounts to a breach, even if it would be justified if pursued under legislation. While the practice of filtering is undertaken by New Zealand ISPs, the sites filtered are based on a list created by a government department. There is no section in the FVPC Act which provides the basis for a filter, unless perhaps if the seizure provision of the FVPC Act is read incredibly creatively and broadly.[355] In light of the resistance to do this with other provisions of the statute, such as "publication" and s 3(2), this is probably untenable. The issue of arbitrariness also hangs over the decision to only filter s 3(2)(a) material, instead of all objectionable material.

To mitigate these concerns, filtering should be undertaken explicitly by the state. Or, at least, it should be clear to the public that the filter is applied by the state not by private parties/ISPs. The right to freedom of expression is based solely on the vertical relationship between the state and the individual. The process whereby the New Zealand ISPs are co-opted into the classification scheme and enable a state limitation on the right to free expression, while absolving the state of actual direct responsibility for any rights breach, must amount to a further curtailment of the right and/or a fudging of the vertical and horizontal relationship between citizen and state and citizen and fellow citizen, particularly given the lack of clear avenues for citizens to review any decision to filter. As these parties currently enjoy statutory immunities from liability, the co-opting of ISPs as proxy censors is also problematic.

The rights issue of informal filtering has not been tested by the courts. All the same, formalising this filtering in law is unlikely to be more inconsistent with the right to freedom of expression than the status quo. Filtering would be subject to the constraints of the subject matter gateway, the s 3(2)(a) requirements and the other administrative constraints of the FVPC Act; such constraints would reduce the scope of filtering to only that expression which the New Zealand public does not have a right to. To block Internet expression is a practice approached with caution primarily because the communicative capacity of the Internet is unprecedented and has now become normalised. From a theoretical perspective, this caution is a symptom of the space versus network theory. When the Internet is regarded as a communication medium this caution loses heft. Governments have comfortably blocked large amounts of expression (such as film, video and literature) at bottlenecks created by borders and distribution channels before it reached the public. It is argued filtering Internet publications is about making a mental leap and having the ability to regard both physical expression and Internet expression as synonymous. Alternatively, to do nothing with a system of filtering that

[354] Butler and Butler, above n 3, at [6.12.1].

[355] Film, Videos and Publications Classification Act 1993, s 108.

lacks legal formalisation is more problematic if filtering is here to stay. To continue to operate the filter with legitimacy requires (a) underpinning it with legal authority such as formalisation in statute; (b) broadening the filter to apply to all objectionable expression to limit the perception of symbolic permission of objectionable expression; and (c) signaling clear demarcations as to the legal roles and obligations of the parties involved so as to better engage the public and the industry in their rights and responsibilities. This would likely require some statutory change. For example, the Australian government interpreted s 313 of the Telecommunications Act 1997 (Aust), which requires ISPs to "help as is reasonably necessary" government officials, in such a way that extended the government's powers to order filtering and take down of objectionable content. No such equivalent exists in New Zealand law and if such a law was enacted it would have the benefit of being more targeted and specific.

Lacking the space in this thesis to set out what comprehensive reform would look like, it would still be the case that any statutory basis for filtering would be subject to the rigours of parliamentary process, public scrutiny, the s 7 report of the Attorney-General and, after enactment, the check and balance processes of review and appeal that all powers under the FVPC Act are subject too. For example, if a member of the public wanted to appeal a decision to filter a particular publication they could undertake the appeal process set out in the FVPC Act, something they are currently unable to do because of the lack of capacity in statute to do so. As suggested above, the change would also need to be clear and intelligible, use terms not tied to a particular technology and must take into account the conclusions of the FVPC Act rights jurisprudence.

Sharing the enforcement burden: The myth of mere conduits as a basis for service provider immunity

The next proposal for reform is to repeal s 122 of the FVPC Act. This would potentially expose those parties previously exempt to liability. It is argued that while there may be ideological reasons for only focusing on end users, this reasoning does not account for the commercial evolution of parties further upstream in the Internet transaction. Enforcing the FVPC Act solely against individuals or end users is disproportionate and arbitrary. Exempting a band of potentially culpable parties from liability for objectionable expression also has implications for the right to freedom of expression in that some parties' right to freedom of expression is not limited in the way the right is limited for the rest of New Zealanders. This myopic focus on end users has also hampered enforcement on the Internet, and contradicts the enforcement strategy used when the FVPC Act was first enacted. Without alternative targets of enforcement, other than New Zealand end users, objectionable expression is able to circulate on the Internet in New Zealand unimpeded. This section will show that alternative targets of

enforcement are available, namely Internet service and platform providers, and that there are good reasons for turning our attention to them.

Furthermore, legal immunities such as s 122 of the FVPC Act are based on unsound justifications, regardless of whether you view the Internet as a public sphere or just another communication medium. These parties are no longer mere conduits of information. While repealing s 122 may create uncertainty as to the legal roles and basis for liability for upstream parties, these parties already have the technical mechanisms necessary to meet the requirements of the FVPC Act and avoid their potential liability (even without the protection of s 122). What they lack is the incentive to do so. While there are limitations to exposing these parties to liability, one of them is not the further limitation of the right to freedom of expression. Instead by making these parties accountable to the law, this makes the law's application less arbitrary and more proportionate to the role they play in making expression available in New Zealand. The repeal of s 122 would signal to these parties that if they wish to participate in the availability of expression in New Zealand they must do so based on New Zealand's legal framework.

That individuals are the primary addressees of the statute and the only practical target of enforcement is a product of ideological assumptions about the Internet. Regulators tend to focus on end users because Internet technology has generally developed in order to improve the online experience for end users. Zittrain writes comprehensively on points of control, or the points at which the state can intervene in offending conduct. These could be the source user, the source ISP or the destination user. He suggests that regulating the "middle of the internet" (upstream parties instead of end users) violates the end-to-end principles that were intended by the Internet's engineers and their design.[356] This rigid view prevents regulators from looking into alternative sources of enforcement, particularly parties further upstream and has led to a status quo where "middle-men" on the Internet are exempt from any liability for objectionable expression they may circulate, store or even push onto individuals.

The consequences of this status quo are aggravated in a context where prosecuting those individuals responsible for making and making available objectionable expression is difficult and there are few enforcement strategies available while harm perpetuates online. The model for catching online offenders is no more sophisticated than it was two decades ago. Early attempts involved linking objectionable expression to the source, verifying authenticity (and location for jurisdictional purposes) and placing the burden of liability on "speakers".[357] This

[356] Johnathan Zittrain "Internet Points of Control" (2003) 44 BCL Rev 653 at 687.

[357] Lambers, above n 68, at 114-115.

model is still in practice and if the offending speaker is not a New Zealand individual, the Unit has few available options to address the offending expression. This is despite the fact that the expression has likely passed through a variety of servers and thus "conduits" in order to reach New Zealand servers and screens. Tambini says that the current model (the limited liability, mere conduit, knowledge-based model of Internet content regulation) is more likely designed with private parties in mind and less with the objective of preventing illegal activity.[358] Zittrain says that based on the current model "the regulator must settle for either much leakier enforcement or much more resource-incentive measures that target the individual".[359] No single enforcement agency can police the Internet and the majority of agencies lack the jurisdiction or the political clout to target foreign speakers or their expression that impacts on their local communities. But by not addressing or not being seen to address these parties is problematic, notwithstanding the harm the expression perpetuates on the community. Reed identifies the perception problem where enforcement fails to take action in the cases of foreign parties (and other parties further upstream):[360]

> The statement here is not that the law is unworthy of respect by persons generally, but rather that the foreign actor is not obliged to respect it in particular circumstances. In other words, although the law applies in theory to the foreign actor, in practice the state has informed the actor that it can be ignored.

As Internet use expands, the gap between the law as it applies in theory and in practice will only expand, further undermining the adequacy of the law.

It is significant that not enforcing the FVPC Act against foreign and upstream parties is in contradiction to the enforcement strategy used when the statute was enacted. The Unit and its predecessors would effectively target upstream parties such as publishers and distributors before publications reached ordinary New Zealanders. The Internet has disrupted the traditional media/content distribution model and by proxy the enforcement strategy. However, if it was intended that the statute would no longer apply to parties further upstream (such as distributors) this should have been well signalled to industry and individuals. Instead, disruption of the enforcement strategy has happened tacitly and over a relatively short period on the timeline of New Zealand state censorship. The climate where targeting individuals is difficult and upstream parties are permitted to make available objectionable expression on their

---

[358] Tambini and others, above n 72, at 9.

[359] Johnathan Zittrain "Perfect Enforcement" in *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing, Oregon, 2008) 125 at 131.

[360] Reed, above n 228, at 41.

services and platforms (exempt as they are from any responsibility for any third party content) is a climate of market and regulatory failure. Targeting these parties instead of solely focusing on end users would increase the spread of the enforcement burden while expressing the purpose of the law.

Some of the legal scholarship foresees the end of such legal immunities. Lictman believed early on that while there may be mechanisms to encourage these parties to act responsibly, completely immunising them from liability is not one of them: "no one suggests that, because pedestrians can engage in their own forms of precaution, auto-mobile drivers should be immune from tort liability".[361] Marsden predicts that the tide of legal opinion is also changing in relation to arguments previously used to justify immunity:[362]

> An inadvertent consequence of the network neutrality debate is that ISPs exposed themselves as capable of and desirous to search through the content that traverses their networks. Not only did ISPs lose the network neutrality battle on US grounds, they may well have marked the end of their immunity from liability for offending behavior of users.

Fong raises the possibility that a future court will reject the logic underpinning immunity and conclude that these service providers could have reasonably controlled the published statements through new, more advanced software which enables content-screening.[363] Reed suggests that "blanket immunities may in the long term be seen to be a temporary expedient".[364] New justifications will have to be advanced if such legal immunities are to persist in the law. Levmore further suggests that absolute immunities could only be justified where "Internet providers to do their best to reveal or make available the identity of speakers".[365]

Recent legislative action suggests that New Zealand legislators are also sympathetic to this change. Section 24 of the Harmful Digital Communications Act 2015 heralds a movement away from absolute legal immunity for upstream parties. The section puts obligations on online content hosts to actively protect themselves from liability through a series of notification procedures. Section 25 also puts further qualifications on the circumstances in which an online content host can seek protection from liability. Compare this to the FVPC Act

---

[361] Douglas Lichtman "Holding Internet Service Providers Accountable" (2004) 27(4) Regulation 54 at 59.

[362] Marsden, above n 107, at 62.

[363] Adrian Fong "Dissemination of libel by online social platforms: reinterpreting laws to meet the information age" (2014) 25 ICCLR 39 at 42.

[364] Reed, above n 228, at 271.

[365] Levmore, above n 59, at 62.

where it is not the case that these parties must actively protect themselves from liability, "do their best to reveal or make available the identity of speakers" or even take down objectionable expression on their platforms. In sum the persistence of s 122 is out of step with more progressive law and is an unjustifiable exemption that burdens enforcement and undermines the adequacy of the FVPC Act.

Much of the objectionable expression made available on the Internet in New Zealand comes from foreign sources. In lieu of the difficult pursuit of foreign parties and the issues of jurisdiction raised earlier, a plausible alternative target of enforcement must be found. But who to target? Swire's "elephants and mice" theory identifies the variables that make some targets more viable than others. Swire explains that "elephants" are large companies with "thick skin" who are impossible to hide and thus must heed the authority of lawmakers in states where they wish to operate.[366] "Mice", meanwhile, are small mobile actors that can reopen immediately after being kicked off servers and move offshore; they disguise their identity, dispute jurisdiction and hide their assets; "hidden in crannies of the network" they are the greatest challenge to traditional enforcement. Swire suggests that there are already "four significant filters" that resolve this issue of who to target before any court needs to attend to the question. These filters are: technical filters, lack of jurisdiction over defendants, harmonized law and self-regulatory systems.[367] The legal problems that make it through all four of these filters are typically those involving "elephants", where there is little legal harmonization (because of, for instance, moral, social or constitutional differences) and where certain transactions are uniquely structured.[368] The censorship of objectionable expression on the Internet in New Zealand is one of the cases which makes it through all of Swire's "four significant filters". The media/content distribution market is made up of elephants, censorship is an area of law where there is little legal harmonisation internationally and preventing the availability of objectionable expression requires unique mechanisms. Swire is of the view that in such cases states should go after "alternative targets of enforcement" such as ISPs. As "mice" typically base themselves in lower risk jurisdictions and avoid higher risk jurisdictions, while still being able to perpetuate harm on a local population, Swire believes that attributing liability to more reachable ISPs is the better means of achieving compliance.[369]

[366] Peter P Swire "Elephants and Mice Revisited: Law and Choice of Law on the Internet" (2005) 153 University of Pennsylvania Law Review 1975 at 1979.

[367] At 1976.

[368] At 1993.

[369] At 1982.

This thesis argues that there are six reasons for regulating upstream actors such as Internet service and platform providers. Some reasons will already be evident, others will be expanded upon. The reasons are as follows:

(a) Other comparable states have implicated upstream parties in censorship practices or made them liable. As a result, to do so in New Zealand would not be anomalistic. Rather, it would reduce the likelihood of New Zealand becoming a safe harbor for "mice" and align with the emerging paradigm.
(b) A limited number of parties control access to the Internet and there are significant barriers to entry in the market (an individual cannot just set up their own ISP). Like any other market where its participants have a tendency towards monopolistic behavior, they should be regulated, particularly so because expression is valued as a fundamental democratic good.
(c) Upstream parties create bottlenecks in the network (this is more likely with increased vertical integration). This is not only the easiest point of control but the most viable enforcement alternative to targeting end users.
(d) Many of these parties have already set up enforcement mechanisms based on their own terms of service and community standards so have demonstrated that censorship of their services is a standardised practice.
(e) Most importantly, and key to their unique position in the marketplace, is that these parties hold the wealth of key data which is required to identify and prosecute offending end users, quite unlike any pre-existing mass media/communication industry player or mere conduit utility provider.

Whether or not to regulate upstream parties depends on which approach to the Internet is adopted. If the Internet is a public space then those that provide access to it play a significant public role in provision of access to that public space. What follows is that they must be regulated like any other public utility provider. If this approach is the basis for their liability (or lack thereof) under the FVPC Act, then it must be applied consistently in all other areas of the law for the law to have integrity. Consistency would require a revision of the hands-off approach which the state has taken to issues such as discriminatory practices by ISPs and extreme convergence of vertical online services. Importantly, if the Internet is a public utility, Internet service and platform providers have public interest obligations. Specifically with regards to expression, decisions that affect an individual's right to freedom of expression, including the freedom to seek, receive, and impart information and opinions of any kind in any form on the Internet, would need to be subject to judicial review and other public accountability mechanisms.

Conversely, if the Internet is just another communication medium and these parties are private parties in private transactions, then they must be subject to the law in the same way that private individuals are. The effect of s 122 is to create an exception to a band of offending that all other New Zealanders are subject to, arbitrarily elevating these parties above the law. This exception is no longer based on valid justifications. Section 122 implies that ISPs cannot or do not act in a way that privileges anyone's access to expression. Further, it implies that they cannot probe the "private" data travelling on their networks and certainly cannot non-consensually lift information from this data to sell on and monetise. These assumptions no longer hold true (if they ever did). Lambers rightly criticises the prevalence of the "myth or cliché" that users are unhindered publishers and that middle-men merely control access or edit information streams.[370] The exemption is thus further undermined by the fact that these ISPs actively censor and filter expression on their own volition, and this is either overlooked or endorsed by the state. Though these ISPs consistently demonstrate that they can and do censor expression, and therefore absolutely are not mere conduits of services, this has not resulted in a revision of the justifications that underpin their legal immunity under the FVPC Act.

The repeal of s 122 may result in uncertainty as to how these parties should define their role in relation to the making available of objectionable expression. Rather than relying on outmoded analogies, comparing these parties to industries of old, the more convincing position, as argued by Reed, is that online service providers are often "sui-generis", having no offline equivalent, and thus to draw parallels risks inaccurately representing their legal roles.[371] Suggesting that they are like a publisher, an owner of a notice board, or an importer of the expression is of limited value and their liability should not be designed with these old analogies in mind. This does not mean that these parties should have a new role carved out for them, which would be fertile ground for new exceptions to be made. Rather it would be more principled to treat them as any other party on the Internet. Thus subject to the other recommendations made in this thesis, if a party deliberately made available, or became aware that a third party was using their service or platform to make available objectionable expression (and continued to permit it), they may be subject to the offences under the FVPC Act.

A more acute issue is how parties would know they have exposed themselves to liability under the FVPC Act, particularly the elephants: multinational media/content distributors. Smith recasts this liability paradigm as an exercise in determining where they "sit on the spectrum between country of origin and country of destination".[372] One view favours an actor only being

[370] Lambers, above n 68, at 105.

[371] Reed, above n 117, at 271.

[372] Smith, above n 276, at 936.

liable for Internet offending in its home jurisdiction while the other view favours an actor only being liable in the jurisdiction of the alleged victim. Part of this exercise requires considering the laws of multiple jurisdictions, as online parties typically have global reach. The targeting approach, equally, involves scrutinizing the conduct of the party to then assess if it intended to target a particular jurisdiction and thereby become subject to its laws and liable for the content it carries. As discussed, the targeting approach is favoured by a number of scholars. Schultz suggests that it is more "foreseeable" and provides a "higher threshold" for the link between the private actor and the law:[373]

> While information flows in irrespective of which approach is adopted, accepting targeting means that if an ISP does not narrow down the geographical scope of the information flow produced, it should be deemed to seek the benefits of this global reach, and thus legitimately be exposed to the risks associated with it … including the regulation of those countries.

Timofeeva similarly suggests that going after providers who target the jurisdiction is reasonable because "their actions may also significantly contribute to availability of Internet content to the user".[374] This puts the onus on the party to consider the nature of the expression they carry and ensure it complies before targeting their services to a particular state. Thus there are well tested judicial tests for making a determination as to whether or not a party has exposed themselves to liability which could be adopted into New Zealand law without breaking new ground.

Removal of the protection of s 122 may result in a higher burden on parties further upstream to take active steps such as monitoring and/or take down, as they are likely to be liable for objectionable expression in a way that they would not previously have been. But this simply more accurately reflects the contemporary distribution model and is in proportion to the capabilities of these parties. Service providers and/or platforms have revealed they are able to look into the data of their users, and have mechanisms in place for dealing with non-compliant use. Many of these service providers' terms of use reflect some legal standards and include what use amounts to breaches of those terms. They have a variety of means of punitively dealing with those that abuse their terms. For instance, a breach might result in "(1) execution against some asset made available as a security, such as a bond posted by a member of a networked community or intellectual property left within the community; and (2) expulsion or

[373] Schultz, above n 62, at 818.

[374] Timofeeva, above n 106, at 129.

exclusion from the community".[375] Other consequences include throttling and disconnection or limiting the service in some way: "[s]uspending the account would take place at the physical layer in that the ISP would remove permission for the user to connect to the Internet via their services and cannot therefore be circumvented through the use of code".[376] These are the most effective mechanisms of dealing with offending activity online and it is these mechanisms that states specifically lack. The regulatory disconnect is striking: these parties are able to avoid liability when they are the ones with the technical means to identify offenders and enforce the law.

In theory a wider net of parties subject to liability may result in a chilling effect but in reality this would likely just shift already entrenched goalposts rather than amount to a further limit on the right to free expression. New Zealanders have come to expect that there are terms and conditions that constrain their expressive behaviour on whatever platform or service they are using; this is the nature of their Internet experience by default. Indeed, it has been suggested that there is a popular consciousness with respect to how users view these service providers, specifically that the providers know everything about customers' data and that they are in "cahoots" with law enforcement and corporate power. Kohl considers that this provides an opportunity for cross-fertilisation of interests (regulation and business), as new data frameworks that commercialise data help detect copyright and expression offences. Put another way, "if the watchtower is built, why let it go to waste?"[377] In any event, knowing what these upstream parties are legally able and unable to do may empower New Zealanders, individually and collectively, to assert their rights more confidently and effectively against these parties and the state.

There are limitations inherent to the regulation of upstream parties. Firstly, individuals and states utterly depend on these parties to access Internet technology. The way the technology is developing is likely to intensify this dependence. Zittrain, for example, warns that the appliancisation of the Internet, where users lose the generative capacity of Internet technology such as coding or programming (one of its supposedly democratising qualities) by switching to mobile devices and top-down delivered applications, will amount to a great loss for users

[375] Lodewijk Asscher "Code as Law, Using Fuller to Assess Code Rules" in *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing, Oregon, 2008) at 85.

[376] Michael Filby "Code is Law: Assessing Architectural File Sharing Regulation in the Online Environment" (2013) 8 J Int't Com L & Tech 81 at 100.

[377] Uta Kohl "The rise and rise of online intermediaries in the governance of the Internet and beyond—connectivity intermediaries" (2012) 26 International Review of Law, Computers & Technology 185 at 204.

and inhibit their ability to be part of the discourse about the future of the technology.[378] Another limitation is the difficulty for users and law enforcement to retrieve data intelligibly from the services themselves; to do so depends entirely on the "provider's cooperation".[379] Access to physical hardware in a single location is not likely to be sufficient to retrieve the data necessary to account for all the facts of a legal dispute in the near future. Many other comparable countries (Australia, the EU) have data retention laws that force ISPs and other service providers to disclose the necessary information to catch third party offenders. In New Zealand, no such laws exist, and although ISPs have informal relationships with enforcement agencies, there is no standardisation, legal authority and thus no guarantee that enforcement agencies are able to access necessary information even to investigate offending in New Zealand. This is not only out of step with other comparable countries but is a product of New Zealand's aggrandisement of IPSs. The lack of transparency around these parties' censorship, monitoring or data harvesting practices further hinders regulators' ability to dictate rules.

Exposing these parties to liability under the FVPC Act is likely to further threaten the already precarious compliance relationship. This means that, at the outset, the likely success of exposing these parties to liability will depend on their willingness to participate in the regulatory conversation. This throws up concerns about the power dynamics of the Internet services market. Tambini warns that "those wishing to see ISPs regulate their content should be careful what they wish for—they may find that the economic incentives to police the content outweigh the child protection and free speech arguments".[380] The privatisation of enforcement services with financial bottom lines rather than public service remits may have a raft of negative social consequences not anticipated when legislating or otherwise regulating ISPs. Marsden warns:[381]

> 1) Larger companies are better able to bear compliance costs; 2) larger companies have the lobbying power to seek to influence regulation; and 3) dominant and entrenched market actors in regulated 'bottlenecks' play games with regulators in order to increase the sunk costs of market entry for other actors, and can pass through costs to consumers and innovators in non-competitive markets.

Marsden says that larger companies tend to "game" the system in this way, creating additional impenetrable compliance systems and pricing out potential competitors such as smaller

---

[378] Jonathan Zittrain *The Future of the Internet—And How to Stop It* (Yale University Press, United States, 2008) at 116.

[379] Reed and Cunningham, above n 74, at 179.

[380] Tambini and others, above n 72, at 9.

[381] Marsden, above n 107, at 61.

upstarts. These limitations should be borne in mind when considering the wider practical effect of reform. These parties have a significant impact on the regulation of expression and the Internet user's experience. The vertical integration of these services and further market concentration is unlikely to result in any disruption to the power and influence of these parties. Although unable to be addressed in the space of this thesis, a more viable solution is therefore likely to be one that looks beyond punitive regulatory responses. This does not mean excluding service providers from change to the statutory scheme, but providing incentives as well as using penalties where necessary to achieve compliance. Exempting service providers under the FVPC Act only further distances these upstream parties from their potential regulatory role. There are numerous regulatory schemes that rely on key stakeholder cooperation and so involve them actively in decision making and compliance measures. Features of such schemes that could apply to the FVPC Act include: engaging service providers early in the process of statutory change, giving them an active, resourced and supervised role in the compliance and enforcement scheme (such as monitoring and reporting), and giving them confidence in the fair and just procedures for reviewing decisions and holding offenders accountable. There is even potential for a role in administrative decision making, particularly if the public service role ideology remains entrenched. As many service providers have censorship procedures and mechanisms in place, reform such as this would transition this private censorship practice into something more public, transparent and accountable.

VII The status quo: careening towards post-state regulation

This thesis has argued that the FVPC Act is capable of being an adequate legal framework that applies to online expression. However, the weaknesses and inadequacies of the statute threaten this. The legal framework is not likely to be fit for purpose if the technology develops any further beyond the statute's reach. This is concerning. If the harms which the law aims to prevent are still operating in society, it is not sufficient that those bound by the law no longer comply and the state does nothing as its regulatory position peters out. Reform is the solution. This thesis suggests a starting point for reform would be to: address the language of the statute (with specific amendments proposed), address how Internet filtering is undertaken and how to make this practice more rights consistent, and finally to address the role played by ISPs and other service providers in making expression available (firstly, by doing away with broad unjustifiable immunities). The reforms proposed are not the panacea needed to address all of the weaknesses and inadequacies of the statute. They offer solutions to more basic questions as to what expression the law aims to address, what behaviour it seeks to criminalise and who is subject to the law. More needs to be done in this area to address the range of challenges the Internet poses to the regulation of expression.

As to the rights-consistency of the proposals, this thesis will not expand the powers of the FVPC Act. In accordance with the conclusions of the rights jurisprudence, the gateway provisions of the FVPC Act (s 3 specifically) will not be changed and will continue to act as a constraint on the scope of the statute. In practice the changes may lead to more expression being captured and classified in accordance with the law, as the law intended when it was enacted and affirmed by subsequent amendments, but this may not ultimately result in more expression being restricted. Further, as the courts have deemed that New Zealanders do not have a right to objectionable expression, if more of this type of expression is captured and banned, the right is not burdened further by the changes proposed. Importantly, if (as a result of these changes) the law is clear and intelligible, if the public and industry understand how it applies to them, and therefore better understand what their expressive rights and responsibilities are, this is likely to increase their engagement with their expressive rights. Finally, a transparent and accountable framework vested in the public interest of New Zealanders is likely to be a less restrictive alternative to the censorship frameworks of private (foreign) companies.

The pivotal issue is that the Internet has not radically undermined private interests (rather transformed them) but has the potential to undermine the public interests of states who do not assert their legal dominion. May suggests that "the 'information age' both enhances the power of states that can effectively control their jurisdiction, and contributes to the weakness of those that do not".[382] There is currently a gap between the law and technology where uncertainty festers. There are no incentives for the technical community and foreign parties wishing to and operating in New Zealand to wait for lawmakers to fill this gap when there is an enthusiastic population willing and able to use their services, even illegally. Kirby is of the view that a lack of regulatory action, such as reform to fill such gaps, should not be perceived as serendipitous:[383]

> At one time we must accept that doing nothing to regulate technology involves making a decision… To do nothing is therefore effectively to decide that nothing should be done. It does not necessarily amount to a decision to wait and see.

For New Zealand, to do nothing is to engineer deregulation by default. Deregulation will only create a regulatory vacuum. A state's faith in the corrective power of the market or technology is not likely to be rewarded and will lead to cosmetic regulatory "fixes" being tacitly built into

[382] C May "Commodifying the 'information age': Intellectual property rights, the state and the Internet" 1(3) (2004) SCRIPTed 408 at 419.

[383] Kirby, above n 321, at 318.

technology by technologists and, as Tavini believes, to the detriment of traditional means of debating public policy.[384] Reidenberg argues that ceding law-making to technologists in this way negates the state's role in securing rights for its citizens and that the state must set the public policy and let the technology follow, not the other way around.[385] Private corporations, instead of individuals or their elected representatives, will determine individuals' ability to seek, receive, and impart information and opinions of any kind, via contracts outlining terms of use and "community standards". Tambini rightly questions why "we" are abandoning public law—to solve regulatory gaps—in lieu of solutions derived from contract law.[386] The logical conclusion to the lack of reform is the flat cessation of New Zealand law-making authority, which will, in practice, fall to the Internet monoliths that rule by terms of service. This goes to the question (which is outside of the scope of this thesis) of whether the state is under a positive obligation to ensure citizens' rights and resist the encroachment of technologists' rule of law.

A future without legal frameworks amounts to a weakened relationship between citizens and the state and fewer opportunities to redress rights violations against private entities. New Zealanders will have to resign themselves to an Internet experience where: (a) harm on the Internet is to be managed by individuals without intervention by the state and (b) technology, technologists and thus private interests alone will determine what rule-sets guide behaviour. What will the implications of this new (lawless) order be for the right to freedom of expression? Certainly the state will no longer be able to restrict a person from receiving information that others can and are willing to impart. However all of New Zealand's legal frameworks including rights jurisprudence would be eclipsed. Instead, expressive *rights* will be based entirely on a horizontal (and contractual) relationship. What's more, individuals are likely to comply with the wholly unbalanced contracts presented to them by Internet service and platform providers even if compliance is not required of them by their own national laws (where those laws still apply) and even where there is no risk of sanction if they do not comply. This phenomenon is described as the "Amazon paradox"[387] or as a by-product of the "locked in user".[388] The size and convenience these networks provide often outweighs the dissatisfaction of disparate individual users and thus these rule-sets are implemented with impunity. That individuals are willing to disclaim their own national rights, or are apathetic to them, in exchange for mere access to online services demonstrates the powerful influence of the Internet and those that provide access, platforms and services on it.

---

[384] Einar Himma and Tavani, above n 325, at 44.

[385] Reidenberg, above n 328, at 182.

[386] Tambini, above n 72, at 276.

[387] Reed, above n 75, at 77.

[388] Wu, above n 67, at 276.

Further, while laws can be amended and executive decisions can be reviewed, these contractual rights will only be subject to the whims of corporate hierarchy. Contractual *rights* are unlikely to be negotiated in any democratic way, particularly given the lack of bargaining power individuals have against these multi-national entities. Individuals are disadvantaged by this as they cannot know what human rights will be acceded to by the provider and as they are already in a position where it is rare to litigate or enforce their national law, rights, or customs against Internet companies. Under these conditions, individuals' democratic identity and agency is reduced. But this should not be surprising. Democracy is not the core objective of these services and platforms, and self-fulfillment is realised only to the extent of the predilection of the Internet company in question. In a context where access to the Internet is increasingly necessary for an individual to engage democratically, private censorship by blocking, throttling and disconnection takes place irrespective of users' human rights. Ultimately, if the "marketplace of ideas" truly is a market, the dominant idea or opinion that emerges will not be the most objective truth but the most profitable truth.

To their credit, these companies may acknowledge or make provision for human rights but they certainly do not owe duties and responsibilities to individuals, in the same ways the state does. This is the core of Laidlaw's thesis on the corporate social responsibility of Internet companies:[389]

> … reliance on self-regulatory frameworks without guidance on how companies can meet their human rights responsibilities results in a governance gap, the very act of strengthening their self-regulatory free speech structures risks dissuading companies or industries from addressing free speech concerns for fear of incurring direct liability.

Corporate free speech structures are unlikely to bear any resemblance to New Zealand's right to freedom of expression and what New Zealanders have come to expect as a right that they are protected by. Any concerns over (a) the lack of clarity as to the extent the right's protection, (b) what amounts to a justifiable limitation and (c) the institutional discretion of classification bodies, are augmented in a context of corporate free speech structures. Joseph hesitantly suggests that there may be precedent for the application of NZBORA in private actions (using the example of *Lange v Atkinson*), where the courts have considered and applied the Bill of Rights to common law actions between private individuals.[390] But even if that could be argued in a case against a censorious Internet company, it is not at all a solid foundation upon which

[389] Laidlaw, above n 330.

[390] Joseph, above n 30, at [128].

to guarantee speech rights. This is particularly urgent if it is non-New Zealand parties determining the rules. It is this more tacit erosion of rights and responsibilities, where individuals take their rights for granted, that is most insidious to a democratic culture, as Hardie Boys J has said:[391]

> In contemporary New Zealand society the importance of human rights can go unappreciated. They may be taken for granted; they may be seen as irrelevant; other considerations, such as expediency or alarm or outrage may suggest they should be overridden. Perhaps it is only when they are abrogated that their crucial role in ameliorating the human condition is truly appreciated.

Given the dramatic effect the Internet has on the New Zealand experience, to give up on our national legal frameworks (including rights frameworks) for this technology would mean a significant human rights dissolution overall, one that the state as an embodiment of the public interest cannot afford to take for granted.

Ultimately, foregoing reform of the FVPC Act—one of the last legislative abatis between the New Zealand public and objectionable expression—amounts to an abrogation of the state's long-standing goal of protecting children and other vulnerable groups. We cannot assume corporate interests left to rule the Internet will prioritise this goal in the same way the state is obliged to. There are, as Kohl suggests, good reasons why national laws come in all shapes and sizes, reflecting the peculiar political, cultural, and social values of States and their communities.[392] For all its idiosyncrasies, New Zealand law is a product of its complex political, legal and social value systems. An algorithm, conversely, cannot account for the nuance of norms, laws, values and policy of a community, nor the myriad of communities that exist online or in the real world. It is certainly not answerable to transparency, accountability and review mechanisms. Instead, if we can all agree that free expression (subject to justified limitations) is a pillar of New Zealand identity, then it follows that technology which enables expression must accord with our law and be subject to corresponding legal constraints. The proper basis for censorship is not a private company's "accept" icon on an electronic terms of service policy (from a far off jurisdiction), but a robust legal framework, made up of laws which are able to be understood by those to whom they are addressed and which reflect the burden of liability and enforcement proportionately.

---

[391] *Ministry of Transport v Noort* [1992] 3 NZLR 260, (1992) 8 CRNZ 114 at 141.

[392] Kohl, above n 244, at 257.

BIBLIOGRAPHY

Cases

Batty v Choven (2005) 23 CRNZ 214, [2006] NZAR 127.

Department of Internal Affairs v Merry [2000] DCR 733.

Department of Internal Affairs v Young [2004] DCR 231.

Dixon v R [2015] NZSC 147.

G (CA741/11) v R [2012] NZCA 152.

Goodin v Department of Internal Affairs [2003] NZAR 434.

Hansen v R [2007] NZSC 7, [2007] 3 NZLR 1.

Hosking v Runting [2005] 1 NZLR 1.

Internal Affairs Department v Benning DC Dunedin CRN 7012018045, 12 March 1998.

Kellet v Police (2005) 21 CRNZ 743.

Living Word Distributors Ltd v Human Rights Action Group (Wellington) [2000] 3 NZLR 570.

Meyrick v Police HC Hamilton CRI-2005-419-000058, 31 July 2007.

Ministry of Transport v Noort [1992] 3 NZLR 260.

Moonen v Film and Literature Board of Review [2000] 2 NZLR 9.

Moonen v Film and Literature Board of Review [2002] 2 NZLR 754.

Murray v Wishart [2014] NZCA 461, [2014] 3 NZLR 722.

New Zealand Post Ltd v Leng [1999] 3 NZLR 219.

O'Brien v Brown [2001] DCR 1065.

R v Clarke [2012] DCR 425.

R v Cox [1990] 2 NZLR 275.

R v D (CA 287-2010) [2011] NZCA 69.

R v Hayes (2006) 23 CRNZ 547.

R v Millward [2000] DCR 633.

R v Schaper DC Christchurch, 21 April 2008.

R v Spark [2009] NZCA 198.

R v Spark [2009] NZCA 345, 3 NZLR 625.

Rafiq v Google New Zealand Ltd [2014] NZHC 551.

Shaw v Department of Internal Affairs [2005] DCR 898.

Spark v R [2009] NZSC 130.

Stewart v Department of Internal Affairs [2014] NZHC 2209.

University of Newlands Ltd & Anor v Nationwide News Pty Ltd (2004) 17 PRNZ 206.

France

UEJF & LICRA v Yahoo! Inc. & Yahoo! Tribunal de grande instance [TGI] [ordinary court of original jurisdiction] Paris, 22 May 2000, (Fr).

United Kingdom

Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors [2016] EWCA Civ 658.

United States of America

Brown v Entertainment Merchants Association 564 US 08-1448 (2011).

Comcast v Federal Communications Commission 600 F 3d 642 (DC Cir 2010).

Yahoo! Inc v La Ligue Contre le Racisme et l'Antisemitisme (LICRA) 169 F Supp 2d (ND Cal 2001).

Zeran v America Online Inc 129 F 3d 327 (4th Cir 1997).

Legislation

Broadcasting Act 1989.

New Zealand Bill of Rights Act 1990.

Films, Videos, and Publications Classification Act 1993.

Copyright (Removal of Prohibition on Parallel Importing) Amendment Act 1998.

Crimes Amendment Act 2003.

Criminal Procedure Act 2011.

Copyright (New Technologies) Amendment Bill 2008.

Harmful Digital Communications Act 2015.

Unites States of America

Obscenity 18 USC § 1460-1470.

Books and Chapters in Books

Lodewijk Asscher "Code as Law, Using Fuller to Assess Code Rules" in Brownsword and Yeung (eds) *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing, Oregon, 2008).

Eric Barendt *Freedom of Speech* (2nd ed, Oxford University Press, New York, 2005).

Roger Brownsword "So What Does the World Need Now? Reflections on Regulating Technologies" in Brownsword and Yeung (eds) *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing, Oregon, 2008).

Roger Brownsword *Law and the technologies of the twenty-first century: text and materials* (Cambridge University Press, Cambridge, 2012).

Butler and Butler *The New Zealand Bill of Rights Act : a commentary* (2nd ed, LexisNexis NZ Ltd, Wellington, 2015).

Ursula Cheer *Burrows and Cheer Media Law in New Zealand* (7th ed, LexisNexis NZ Ltd, Wellington, 2015).

Deibert and others (eds) "Australia and New Zealand" in Deibert (ed) *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace* (MIT Press, United States, 2010).

Deibert and Rohozinski "Beyond Denial" in Deibert (ed) *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace* (MIT Press, United States, 2010).

Hans Fischer "Technology Perspectives on Code" in Dommering and Lodewijk Asscher (eds) *Coding regulation: essays on the normative role of information technology* (T. M. C. Asser Press, The Hague, 2006).

Alisdair A Gillespie *Child Pornography: Law and Policy* (Routledge, New York, 2011).

Judge David Harvey *internet.law.nz* (3rd ed, LexisNexis NZ Ltd, 2011).

Grant Huscroft and others *The New Zealand Bill of Rights Act: A Commentary* (Oxford University Press, Australia, 2006).

Phillip A Joseph (ed) *Constitutional & Administrative Law in New Zealand* (online looseleaf ed, LexisNexis).

Yvonne Jewkes "The Private Policing of Internet Crime" in Jewkes and Yau (eds) *Handbook of Internet Crime* (Routledge, United States, 2011).

Michael Kirby "New Frontier: Regulating Technology by Law and 'Code'" in Brownsword and Yeung (eds) *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing, Oregon, 2008).

Uta Kohl *Jurisdiction and the Internet: Regulatory Competence over Online Activity* (Cambridge University Press, Cambridge, 2007).

Emily B Laidlaw *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility* (Cambridge University Press, United Kingdom, 2015).

Rik Lambers "Speech Control through Network Architecture" in Dommering and Lodewijk Asscher (eds) *Coding regulation: essays on the normative role of information technology* (T. M. C. Asser Press, The Hague, 2006).

Mark Levene *Introduction to Search Engines and Web Navigation* (2nd ed, John Wiley & Sons Inc., New Jersey, 2010).

Saul Levmore "The Internet's Anonymity Problem" in *The Offensive Internet: Speech, Privacy and Reputation* (Harvard University Press, 2011).

McIntyre and others "Internet Filtering" in *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing, Oregon, 2008).

Milton Mueller *Networks and States: The Global Politics of Internet Governance* (MIT Press, Cambridge, 2010).

Andrew Murray *The Regulation of Cyberspace: Control in the Online Environment* (Routledge-Cavendish, United Kingdom, 2007).

Nart Villeneuve "Barriers to Cooperation" in Deibert and others (eds) *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace* (MIT Press, United States, 2010).

Chris Reed *Internet Law: Text and Materials* (2nd ed, Cambridge University Press, UK, 2005).

Chris Reed *Making Laws in Cyberspace* (Oxford University Press, Oxford, 2012).

Reed and Cunningham "Ownership and Information in Clouds" in Christopher Millard (ed) *Cloud Computing Law* (Oxford University Press, Oxford, 2013).

Jeffrey Rosen "The Deciders: Facebook, Google and the Future of Privacy and Free Speech" in Rosen and Wittes (eds) *Constitution 30: Freedom and Technological Change* (Brookings Institution Press, United States, 2011).

Graham JH Smith *Internet Law and Regulation* (4th ed, Sweet & Maxwell, London, 2007).

Cass Sunstein *Democracy and the Problem of Free Speech* (The Free Press, United States, 1993).

Tambini and others *Codifying Cyberspace: Communications self-regulation in the age of Internet convergence* (Routledge, United Kingdom, 2009).

Tim Wu "Is Filtering Censorship? The Second Free Speech Tradition" in Rossen and Wittes (eds) *Constitution 30: Freedom and Technological Change* (Brookings Institution Press, Washington, 2011).

Karen Yeung "Towards an Understanding of Regulation by Design" in Brownsword and Yeung (eds) *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing, Oregon, 2008).

Peter Yu "Towards the Seamless Global Distribution of Cloud Content" in Cheung and Weber (eds) *Privacy and Legal Issues in Cloud Computing* (Edward Elgar Publishing, United Kingdom, 2015).

Johnathan Zittrain "Perfect Enforcement" in *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing, Oregon, 2008).

Jonathan Zittrain *The Future of the Internet -- And How to Stop It* (Yale University Press, United States, 2008).

Journal Articles

Jack M Balkin "Old-School/New-School Speech Regulation" (2013) 127 Harv L Rev 2296.

Jessica E Bauml "It's a Mad, Mad Internet: Globalization and the Challenges Presented by Internet Censorship" (2010) 63 Fed Comm LJ 697.

Roger Brownsword "The shaping of our on-line worlds: getting the regulatory environment right" (2012) 20 International Journal of Law and Information Technology 249.

Anupam Chander and Uyen P Le "Free Speech" (2014) 100 Iowa L Rev 501.

Johnathan Clough "A world of difference: the Budapest Convention on Cybercrime and the challenges of harmonisation" 40 Monash University Law Review 698.

Kenneth Einar Himma and Herman T Tavani "Regulating cyberspace: concepts and controversies" (2007) 25 Library Hi Tech 37.

Clive Elliot “The Napster Saga” [2001] NZLJ 297.

Michael Filby “Code is Law: Assessing Architectural File Sharing Regulation in the Online Environment” (2013) 8 J Int’t Com L & Tech 81.

Adrian Fong “Dissemination of libel by online social platforms: reinterpreting laws to meet the information age” (2014) 25 ICCLR 39.

Andrew Geddis “The state of freedom of expression in New Zealand: an admittedly eclectic overview” (2008) 11 Otago L Rev 657.

Alisdair A Gillespie “Jurisdictional issues concerning online child pornography” (2012) 20 Int J Law Info Tech 151.

Kent Greenawalt “Free Speech Justifications” (1989) 89 Columbia Law Review 119.

Marjorie Heins “The Brave New World of Social Media Censorship” (2013) 127 Harv L Rev F 325.

Julie L Henn “Targeting Transnational Internet Content Regulation” (2003) 21 BU Int’l LJ 157.

Arne Hintz “Outsourcing Surveillance - Privatising Policy: Communications Regulation by Commercial Intermediaries” (2014) 2 Birkbeck L Rev 349.

Chris Hoofnagle “Free: Accounting for the Costs of the Internet’s Most Popular Price” (2014) 61 UCLA L Rev 606.

Ty E Howard “Don’t Cache out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files” (2004) 19 Berkeley Technology Law Journal 1227.

Gil’ad Idisis “How to Make Lemonade from Lemons: Achieving Better Free Speech Protection without Altering the Existing Legal Protection for Censorship in Cyberspace” (2013) 36 Campbell L Rev 147.

David R Johnson and David Post “Law and Borders: The Rise of Law in Cyberspace” (1996) 48 Stanford Law Review 1367.

Orin S Kerr “The problem of perspective in Internet law” (2003) 91 Georgetown Law Journal 357.

Nancy Kim “Internet giants as quasi-governmental actors and the limits of contractual consent” (2015) 80 Missouri Law Review 723.

Dean Knight “Objectionable Offence: A Critique of the Possession Offence in the Films, Videos, and Publications Classification Act 1993, An” (1997) 27 VUWLR 451.

Uta Kohl "The rise and rise of online intermediaries in the governance of the Internet and beyond – connectivity intermediaries" (2012) 26 International Review of Law, Computers & Technology 185.

Emily B Laidlaw "The responsibilities of free speech regulators: an analysis of the Internet Watch Foundation" (2012) 20 International Journal of Law and Information Technology 312.

Stefan Larsson and others "Law, norms, piracy and online anonymity" (2012) 6 Journal of Research in Interactive Marketing 260.

Douglas Lichtman "Holding Internet Service Providers Accountable" (2004) 27 Regulation 54.

Daithí Mac Síthigh "The mass age of internet law" (2008) 17 Information & Communications Technology Law 79.

Dan Ma "Push or Pull? A Website's Strategic Choice of Content Delivery Mechanism" (2015) 32 Journal of Management Information Systems 291.

Bernhard Maier "How Has the Law Attempted to Tackle the Borderless Nature of the Internet" (2010) 18 Int'l JL & Info Tech 142.

Christopher Marsden "Network Neutrality and Internet Service Provider Liability Regulation: Are the Wise Monkeys of Cyberspace Becoming Stupid?" (2011) 2 Global Policy.

Mark G Materna "Protecting Generation Z: A Brief Policy Argument Advocating Vicarious Liability for Internet Service Providers" (2012) 47 USF L Rev 109.

C May "Commodifying the 'information age': Intellectual property rights, the state and the Internet" (2004) 1 SCRIPTed 408.

Miles McCarthy "Censornet: The Competing Ideals of Censorship and Cyberspace" (1997) 27 Victoria U Wellington L Rev 349.

Janet McLean "The Impact of the Bill of Rights on Administrative Law Revisited: Rights, Utility, and Administration" [2008] NZL Rev 377.

Abhilash Nair and James Griffin "The regulation of online extreme pornography: purposive teleology (in) action" (2013) 21 International Journal of Law and Information Technology 329.

An Nguyen and Mark Western "The complementary relationship between the Internet and traditional mass media: the case of online news and information" (2006) 11(3) Information Research.

Mark O'Brien "The Internet, child pornography and cloud computing: the dark side of the web" 23 Information & Communications Technology Law 238.

Chris Reed "Online and Offline Equivalence: Aspirations and Achievement" (2010) 18 Int'l JL & Info Tech 248.

Chris Reed "How to Make Bad Law: Lessons from Cyberspace" (2010) 73 The Modern Law Review 903.

JR Reidenberg "Lex informatica: The formulation of information policy rules through technology" (1998) 76 Tex L Rev 3 553.

Jacob Rowbottom "To Rant, Vent and Converse: Protecting Low Level Digital Speech." (2012) 71 Cambridge Law Journal 355.

Sallaert and Chen "An Economic Analysis of Online Advertising Using Behavioural Targeting" (2014) 38 MIS Quarterly 429.

Thomas Schultz "Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface" (2008) 19 Eur J Int Law 799.

Scott J Shackelford "Toward Cyberpeace: Managing Cyberattacks Through Polycentric Governance" (2013) 62 American University Law Review 1273.

Richard A Spinello "Code and moral values in cyberspace" (2001) 3 Ethics and Information Technology 137.

John Suler "The Online Disinhibition Effect" (2004) 7 CyberPsychology and Behavior 321.

Peter P Swire "Elephants and Mice Revisited: Law and Choice of Law on the Internet" (2005) 153 University of Pennsylvania Law Review 1975.

Yulia A Timofeeva "Worldwide Prescriptive Jurisdiction in Internet Content Controversies: A Comparative Analysis" (2004) 20 Conn J Int'l L 199.

Barney Warf "Geographies of global Internet censorship" (2011) 76 GeoJournal.

Erik O Wennerstrom and Csaba Sandberg "Combating Cybercrime - Developments in the European Union" (2010) 56 Scandinavian Stud L 247.

Christopher Yoo "The Changing Patterns of Internet Usage" (2010) 67 Federal Communications Law Journal 67.

Georgios I Zekos "State cyberspace jurisdiction and personal cyberspace jurisdiction" (2007) 15 International Journal of Law and Information Technology 1.

Georgios I Zekos "Cyber Versus Conventional Personal Jurisdiction" (2015) 18 Journal of Internet Law 3.

Johnathan Zittrain "Internet Points of Control" (2003) 44 BCL Rev 653.

Theses and Dissertations

J Bayer "Liability of internet service providers for third party content" (Internet Society of New Zealand, Victoria University of Wellington Law Faculty, 2007).

Lilian Edwards “Content Filtering and the New Censorship” (paper presented to IEEE, February 2010) 317.

Judge David Harvey “Recent Developments in On-Line Defamation” (paper presented to NZLS CLE IT & Online Law Conference, May 2015)

Samuel T Mellor “Regulating Online Conduct: Conundrums and Spatial Metaphors in the Wild West” (LLB (Hons) Dissertation, University of Otago, 2011).

Stephen James Thompson “Protecting Legitimate Speech Online: Does the Net work?” (LLB (Hons) Dissertation, University of Otago, 2012).

Yulia A Timofeeva “Censorship in cyberspace: new regulatory strategies in the digital age on the example of freedom of expression” (Doctoral Thesis, Universität, 2005).

Parliamentary and government materials

(2 December 1992) 532 NZPD 12758, 12761, 12764, 12765, 12767.

(23 August 2012) 683 NZPD 4757.

(2 April 2015) 704 NZPD 2891.

Geoffrey Palmer “A Bill of Rights for New Zealand: A White Paper” [1984–1985] I AJHR A6.

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

Government Administration Committee *Inquiry into the Operation of the Films, Videos, and Publications Classification Act 1993 and related issues* (March 2003).

Crown Law *Legal Advice Films, Videos and Publications Classification Amendment Bill Consistency With The New Zealand Bill Of Rights Act 1990* (14 November 2003).

Films, Videos, and Publications Classification Amendment Bill 2003 (91-2) (select committee report).

Supplementary Order Paper 2005 (325) Films, Videos, and Publications Classification Amendment Bill 2003 (91-1).

Ministry of Justice *Regulatory Impact Statement: Addressing Child Pornography and Related Offending* (Wellington, 2 August 2012).

Department of Internal Affairs *Annual Report* (2000).

Department of Internal Affairs *Annual Report* (2007-2008).

Department of Internal Affairs *Annual Report* (2013-2014).

Office of Film and Literature Classification *Annual Report* (1996).

Office of Film and Literature Classification *Annual Report* (1997).

Office of Film and Literature Classification *Annual Report* (2004).

Office of Film and Literature Classification *Annual Report* (2014).

Reports

The Development of Broadband Access in OECD Countries DSTI/ICCP/TISP(2001)2/Final, 29 October 2001 (Telecom and Internet Report).

The World Internet Project New Zealand *The Internet In New Zealand 2013* (AUT University Institute of Culture, Discourse and Communication, Auckland, 2013).

Merja Myllylathi *JMAD New Zealand Media Ownership Report 2014* (AUT University, Auckland, 2014).

Internet Resources

ATVOD “For Adults Only? Underage Access to Online Porn” <http://www.atvod.co.uk/uploads/files/For_Adults_Only_FINAL.pdf>.

Department of Internal Affairs “Common Questions and Answers” <https://www.dia.govt.nz/Censorship-DCEFS-Common-Questions#6>.

Down To The Wire “1989: It Came Without A Manual” (22 July 2015) < http://downtothewire.co.nz/the-beginning-1989/>.

Down To The Wire “1994: The Internet Nightclub” (22 July 2015) < http://downtothewire.co.nz/1994/>.

Google “Google Transparency Report” (2015) <https://www.google.com/transparencyreport/removals/government/?hl=en>.

ICE “What We Do” <http://www.ice.gov/overview>.

Internet NZ “Net Neutrality” (June 2015) <https://internetnz.nz/content/network-neutrality-discussion-document>.

MBIE *Fast Broadband* (11 December 2015) <http://www.mbie.govt.nz/info-services/sectors-industries/technology-communications/fast-broadband>.

OFCOM “OCI Tracker Benchmark Study Q3 2012” <http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/online-copyright/Intro.pdf>.

Office of Film and Literature Classification “Classification In New Zealand” (8 April 2015) <http://www.classificationoffice.govt.nz/about-censorship/new-zealands-censorship-law-the-films-videos-and-publications-classification-act-1993.html> .

Office of Film and Literature Classification “Research: Changing media use and public perceptions of the classification system” (30 June 2016) <http://www.classificationoffice.govt.nz/news/latest-news/research-public-understanding-2016.html>.

Statistics NZ “Household Use of Information and Communication Technology” <http://www.stats.govt.nz/browse_for_stats/industry_sectors/information_technology_and_communications/HouseholdUseofICT_HOTP2012.aspx>.

Russell Brown “Digital media and the internet - Law and regulation” (19 November 2014) Te Ara - the Encyclopedia of New Zealand <http://www.TeAra.govt.nz/en/digital-media-and-the-internet/page-8>.

Southern Cross Cable Network “FAQ” (2012) <http://www.southerncrosscables.com/home/company/faq>.

Southern Cross Cable Network “Overview and Map” (22 July 2015) < http://www.southerncrosscables.com/home/network/overviewandmap>.

Statistics NZ *Household Use of Information and Communication Techonology: 2006* (27 April 2007)

<http://www.stats.govt.nz/browse_for_stats/industry_sectors/information_technology_and_communications/HouseholdUseofInformationandCommunicationTechnology_HOTP06/Commentary.aspx>.

Statistics NZ "Internet Service Provider Survey: 2014" <http://www.stats.govt.nz/browse_for_stats/industry_sectors/information_technology_and_communications/ISPSurvey_HOTP2014.aspx>.

The White House "Net Neutrality" <https://www.whitehouse.gov/net-neutrality>.

YouTube https://www.youtube.com/t/terms <accessed 12/10/15>.

Other Material

Liz Butterfield *NetSafe: The New Zealand Model for Internet (ICT) Safety Education* (2000).

Michael Cavna "'Nobody Knows You're a Dog": As iconic Internet cartoon turns 20, creator Peter Steiner knows the idea is as relevant as ever" (online ed, Washington Post, July 2013)

CNN "How police smashed child porn club" *CNN.com/World* (online ed, United States, 13 February 2001).

Chris Keall "Tax reform: govt should go further and target multinationals' profit-shifting – Spark boss" *The National Business Review* (online ed, New Zealand, 19 August 2015).

Todd Mclay "Tax bill tackles offshore property speculators and online GST" (press release, 8 December 2015).

Simon Moutter "Making convergence a reality" (Telecom press release, 4 April 2003).

Interview with Steve O'Brien, Censorship Compliance National Manager (the author, Wellington, July 2015).

Statistics NZ *Information Technology Use In New Zealand 2001* (Wellington, 2002).