CENSORNET: THE COMPETING IDEALS OF CENSORSHIP AND CYBERSPACE

*Miles McCarthy**

This article examines current measures, both domestic and international, which attempt to censor the emerging technologies of the Internet. The attenuated application of traditional legislative regimes to such technologies is currently limited only by inherent prosecutorial discretion. Recent legislative mechanisms seek to address the anomaly, only to replicate assumptions concerning the modes and sites of liability. The increasing technological convergence of media necessitates more informed and instructive approaches to the institutions and objectives of censorship, a process which involves international considerations.

I INTRODUCTION

> Pornography has proliferated with each new tool, democratising what had been a more elite possession and obsession, spreading the sexual abuse required for its making and promoted through its use.[1]

The Internet, in relieving New Zealand from the "tyranny of geography",[2] has transformed national boundaries into seamless clouds. The current Internet is a global system of co-operating networks, linking multifarious institutions and individuals, "[t]he headless, anarchic, million-limbed Internet is spreading like bread-mould".[3] There is no

---

* This article was submitted as part of LLB (Honours) programme at Victoria University of Wellington.

1 CA MacKinnon "Vindication and Resistance: A Response to the Carnegie Mellon Study of Pornography in Cyberspace" (1995) 83 Geo LJ 1959, 1959.

2 Information and Technology Advisory Group "Impact 2001: How Information Technology will Change New Zealand" http://www.netlink.co.nz/~itag/impact/impact.htm. (Please note that the Universal Resource Locators cited are current as at 12 February 1997, but are subject to change).

3 B Sterling "A Short History of the Internet" http://gopher.eff.org/links.html.

central or co-ordinating body which administers the Internet and no country has universal jurisdiction. As such a national legislature can only exercise effective control over domestic residents and resources.

The adaptive routing capabilities of the Internet mean that information may travel numerous interconnecting paths before reaching its final destination. The inability to nullify a particular route and thus the dissemination of information has lead to the observation that:[4]

> Technology and censorship are often seen as opposing forces in the information age. Current thinking suggests it is almost impossible to control information without at the same time curtailing some of the benefits.

This article attempts an exposition of the current censorship laws in New Zealand in relation to the Internet, and the proposals for reform.[5] The Films, Videos, and Publications Classification Act 1993, currently the governing legislation, and the Telecommunications Act 1987 are examined. The Technology and Crimes Reform Bill 1994, mooted as the second stage of censorship reform in New Zealand, is critiqued. Finally, recent United States legislation and other regulatory proposals are assessed to the extent they provide possible models for developing solutions in New Zealand.

II NEW ZEALAND

A Films, Videos, and Publications Classification Act 1993

The long title to the Films, Videos, and Publications Classification Act 1993 (FVPCA) states that the Act is to "consolidate and amend the law relating to the censoring of films, videos, books, and *other publications*".[6] The title reflects the legislative impetus behind the enactment of the FVPCA; to develop a coherent and unified censorship regime in place of the sporadic coverage offered by the ad hoc development of previous legislation.

---

4 Above n 2.

5 The object of this paper is not to extrapolate the jurisprudence of censorship in New Zealand or pronounce, at least explicitly, on the desirability of censorship. For a supportive assessment, divorced from technical considerations, see JL Caldwell "Pornography - An Argument for Censorship" (1992) 5 Cant LR 171.

6 Emphasis added.

The appearance of consolidation was, however, dispelled early in the legislation's formative process. A ministerial report on the intended Bill[7] stated that:[8]

> While the scope of the draft bill is very wide, it does not and cannot attempt to deal with every form of pornographic representation...some forms of modern technology are not amenable to regulation by way of a classification statute. Examples are the use of computer links, radiocommunications and telecommunication facilities. Any difficulties with the law relating to these media will have to be addressed separately.

The express denouncing of the legislation as providing coverage of non-tangible media, an interpretation consistent with that of the Committee of Inquiry into Pornography,[9] was resonated throughout the Bill's legislative passage. The Ministry of Justice commented, in an interim report, that the previous legislation (the Indecent Publications Act 1993, the Films Act 1993, and the Video Recordings Act 1987) was "designed to govern the circulation and exhibition of printed and visual matter which exists in a tangible form. The bill describes a censorship/classification system which is suited to regulation of such material".[10]

The suitability or otherwise of the FVPCA to encompass digital media arguably turns on the interpretation given to "publication", as defined by section 2 of the Act. For the statute to apply, media must be able to satisfy the term "publication", which is defined as:

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

The definition is exclusive and "extends the scope of the legislation to catch some forms of material representation which are not covered by existing law".[11] The extension provided by the use of the words "other thing" in combination with subparagraph (ii) is

---

7 Which did not materially differ from the enacted legislation.

8 New Zealand Department of Justice *Films, Videos and Publications Classification Bill - Interim Report* (Wellington, April 1993) 4.

9 Above n 8.

10 Above n 8, 1.

11 New Zealand Department of Justice *Censorship and Pornography: Proposals for Legislation* (Wellington, 1990) 4.

semantically and, arguably, practically significant. Potentially all online services currently available provide and/or utilise information recorded or stored and capable of representation by electronic or computer device.

The Ministry of Justice, while recognising "an extended definition of 'publication' that can cover new forms of material representation",[12] suggested the legislation would "catch articles like computer discs and arcade video games",[13] but that the Bill was "a wholly unsuitable vehicle to address the difficult problems associated with...[modern telecommunications] technology".[14] The emphasis in the definition of "publication" on tangible media may be said to colour the overall interpretation and application of the Act, but it is inconsistent with the express words of the definition to impose such an arbitrary restriction. The recognition of computer disks and arcade games cannot be conceptually justified without the inclusion of other digital media storage facilities; whether hard disks, servers, routers, or gateways.

The conceptual anomaly promoted may, however, be permissible when the practical regulation and classification procedures of the FVPCA are considered. The classification of a publication necessitates its submission to the Classification Office where a ruling on its legal status under the Act can be made. The classification procedure presumes a tangible medium which is capable of submission, without which the classification and the subsequent regulation or prohibition of restricted or objectionable material cannot be enforced:[15]

> The regulatory regime described in the bill can work very effectively for material ("publications") that has a physical form. However, quite apart from any other consideration, this system cannot deal with the simple transmission of pornographic images because a determination that the images are "objectionable" cannot be made if there is no physical record of the image that can be classified. The related problems of prevention, detection, and enforcement are, in this context, virtually insuperable.

The isolation of the statute essentially tangible focus does not, however, necessitate precluding the administration of the FVPCA in relation to digital media. The transmission of data necessarily involves the flow of information already stored or recorded. The potential liability under the FVPCA for digital media susceptible to the classification process was acknowledged by the Ministry of Justice, "the mechanisms for seizure,

---

12 Above n 11.

13 Above n 8.

14 Above n 8.

15 Above n 8.

classification, prosecution an disposal could be made to work if a hard copy is available".[16] The significant applicable offence provisions of the FVPCA include sections 123 and 131.

123. Offences of Strict Liability Relating to Objectionable Publications -

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

(a) Makes an objectionable publication; or

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

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

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

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

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

...

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

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

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

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

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

---

16 Above n 8.

The wording of section 123(4)(b) makes it clear that the provision of offences relating to objectionable offences extends to electronic transmission. The ambit of the provision is wide and would include not only the transmission from an individual user but both online and closed networks.[17] The section, while applicable to Internet Service Providers (ISPs)[18] which create and manage content, arguably extends to pure access providers. The definition of supply could be restricted to those ISPs who provide content rather than pure access providers as the latter do not sell content but merely the access to such content. However, it can be forcefully argued that pure access providers are embraced by section 123(1)(e) in otherwise making available, if not distributing, any objectionable publication.

The section is one of strict liability, section 123(3) expressly excludes knowledge or lack of reasonable belief as defences to a charge under the section. The potential liability of ISPs who retain no, or minimal, editorial control is significant.

> 131. Offence to Possess Objectionable Publication -
>
> (1) Subject to subsections (4) and (5) of this section, every person commits an offence against this Act who, without lawful authority or excuse, has in that person's possession an objectionable publication.

The offence of possession of an objectionable publication, if the above interpretation is to be consistent, extends to possession of digital media on computer and telecommunication devices. As argued above, the inclusion of intangible media in such a form that it can be reproduced for classification purposes prima facie poses no insurmountable conceptual or operational barriers. The defining characteristic is that the data must be stored or recorded in a form capable of being legally possessed.

Such a rudimentary analysis must, however, be tempered by the realities of modern telecommunications. The ability to view does not correspond directly with actual physical possession. The caching of data provides the temporary retention of media without the necessity for recording or storing by the end user.[19] The presence of section 123 indicates that section 131 is directed toward protection of the individual and the resultant effects of

---

17 A closed network is one which provides no connection to the Internet.

18 "Internet Service Providers" can be rudimentally defined as commercial entities which charge a monthly fee and offer modem access to computers or networks linked directly to the Internet; and includes larger national commercial online services such as America Online, CompuServe, Prodigy, and Microsoft Network which allow subscribers to access the Internet while providing extensive content within their own proprietary networks.

19 The Department of Internal Affairs considers the issue of whether browsing the Internet is an offence is a moot point, but states, "...if you download objectionable material onto disk you will certainly be committing an offence", see "Pulling the Plug" http://inform.dia.govt.nz/internal_affairs/businesses/grcr_inf/elect_censor.html.

possessing objectionable material. If such a mischief is to be remedied then the extension of possession to include such transient displays would be consistent. The complications of such an approach must necessarily appear immediate; the requisite intention to exercise control (including the degree of control) over the material is arguably not established, and the enforcement of such an offence would be impractical.

The application of the FVPCA to stored or recorded digital media is evidenced by the recent convictions of local Bulletin Board Service (BBS) operators under the FVPCA. The search warrant used in one of these cases indicates the operational extension of the FVPCA into the area of telecommunications:[20]

> ...the following property CD-Roms, Computer disks and tapes, Computers and [their] ancillary [equipment]..., electronic backup devices, computer software, documentation and accounts that relate to the supply of objectionable publications...are being kept for the purpose of being so dealt with as to constitute an offence against section 123 of the Films, Videos, and Publications Classifications Act 1993.

The United Nations Human Rights Committee, in discussing New Zealand's third periodic report on measures taken to comply with provisions of the International Covenant on Civil and Political Rights, stated that: [21]

> ..it was not the job of the State to overreact concerning objectionable material. It was more suitable for the individual to deal with such issues. The definition of objectionable material was so vague it created serious problems. Vague codes did not serve the needs of the society.

Although such sentiments are apparently moot in regard to reforming the FVPCA, they provide a schema for the interpretation of the legislation in relation to the Internet. The FVPCA offence provisions are capable of addressing objectionable content on domestic proprietary networks and other forms of computer and telecommunications hardware. The imposition of absolute liability is arguably unjustified on policy grounds in relation to the temporary storage of content on network routers, and caching servers, without control or knowledge of the material.[22] Further, the mere downloading of information, without more, should not attract the substantial penalties resultant on the enforcement of offence provisions.

---

20 *Department of Internal Affairs v Merry* [1996] DCR 147, 148.

21 UN Docs CCPR/C64/add 10 HRI/CORE/1/add 33. in Sky Network Television Ltd, Submission on the Technology and Crimes Reform Bill, July 1996, 7.

22 The Department of Internal Affairs has stated that content harboured on servers would be subject to liability, the use of the term "harbour" arguably implies knowledge and control over the information, see Department of Internal Affairs "Pulling the Plug" http://inform.dia.govt.nz/internal_affairs/businesses/grcr_inf/elect_censor.html.

B Telecommunications Act 1987

Sections 8 and 8A (the dial-a-porn section) of the Telecommunications Act deal with the use of profane, indecent, or obscene language or suggestions in connection with a telephone station. The latter section omits the section 8 requirement of intentionally offending the recipient, while including the qualifier that the purpose of the use must be the procurement of any pecuniary gain or commercial benefit. Therefore, assuming these sections encompass the technologies under consideration, the altruistic distributor (having neither an intention to offend or pecuniary motive) can act with impunity.

"Telephone station", as defined by section 2(1) of the Telecommunications Act, means "any terminal device capable of being used for transmitting or receiving any communications over a network designed for the transmission of voice communication". The general nature of the definition threatens to embrace, not only computers, but network routers and gateways. Such devices are not intended to store information for extended periods but act as nodes which interconnect networks and route data.[23]

The wording of sections 8(1) and 8A, by including the terms "language" and "suggestion", could arguably extend to the transmission of digital media as "suggestion" in this context impliedly includes more than mere words. However, such a literal interpretation is arguably counter to the overall intention of the sections[24] and the structure of section 8(2)(a):

> ...any telephone station [used] for the purpose of disturbing, annoying, or irritating any person, whether by calling up without speech or by wantonly or maliciously transmitting communications or sounds, with the intention of offending the recipient...

The contrast of speech and the transmission of communications emphasises the latter's broad application. The omission of such language in sections 8(1) and 8A implies that these sections are confined to the conveyance of profanity, indecency and obscenity by voice.

While the above provisions of the Telecommunications Act are arguably not applicable in providing integral regulatory provisions concerning the Internet, the nature of telecommunication networks ensures that certain definitions and provisions have the potential to influence the form and content of proposed legislation, such as the Technology and Crimes Reform Bill.

---

23 The Executive Committee of the Tuia Society and Information Technology Services VUW, Submission on the Technology and Crimes Reform Bill, July 1994, 5.

24 See A Lewis *Censoring New Telecommunications Technology* (Department of Internal Affairs, Wellington, 1989) 22.

C *Technology and Crimes Reform Bill 1994*

Trevor Rogers,[25] on introducing the Technology and Crimes Reform (TCR) Bill, was transparent in his intention that the proposed legislation constituted the second stage of the Films, Videos and Publications Classification Act:[26]

> The politics of this Bill are quite simple. They are to regulate electronic sounds, images and live-pornography shows, and telecommunication and foreign telecommunication services with amendments to the Broadcasting Act, and to deal with proposed foreign satellite services; and then to link all those parts to a standard identical to those of the Films, Videos and Publications Classification Act so that the product of those technological areas can be examined by the classification office and classified as objectionable or acceptable.

Part I of the Bill deals with the creation of offences and penalties relating to objectionable images, sounds and live shows, and for appropriate classification under the tenets of the FVPCA. The governing assumption is that images and sounds are not covered by existing legislation, and more specifically, do not fall within the definition of publication in the FVPCA. Clause 3 adopts the meaning of objectionable as defined by section 3 of the FVPCA for the purposes of the Bill , "as if images, sounds, live shows, programmes, or foreign satellite services were publications under the [FVPCA]".

Clause 6 of the Bill creates the principal offence relating to objectionable sounds and images:

> Subject to section 9 of this Act, every person commits an offence who broadcasts, transmits, communicates, or receives, through or by any broadcasting or telecommunications link or any electronic, light, sound, satellite, or laser transmission whatever, any objectionable image or objectionable sound for pecuniary gain.

The amorphous nature of the clause, evident by the compendious terms used, reflects the desire of the framers to implement a comprehensive regime. The communication of objectionable images or sounds by or through any telecommunications link or similar device clearly encompasses digital media provided using current, and potential, mediums. The offence is one of strict liability, subject only to those exemptions and defences expressly provided for under clauses 9 and 10 of the Bill.

---

25 MP, Howick.

26 NZPD, vol 540, 1342, 1 June 1994.

The exceptions from criminal liability detailed under clause 9 parallel those under the FVPCA. Clause 10(1) provides that:

> It shall be no defence to a charge under section 6 or section 7 of this Act that, the defendant had no knowledge or no reasonable cause to believe that the image, sound, or live show to which the charge relates was objectionable.

The definition of objectionable and the pervasiveness of the proscription threaten the creation of a regulatory environment in which ISPs and users face extensive criminal liability. The Bill makes no attempt to rationally distinguish between parties with editorial control and mere conduits. Clause 10(4) provides a defence to clause 6 where a network operator "had no knowledge or no reasonable cause to believe that the image or sound to which the charge relates was objectionable". A network operator, as defined under section 2 of the Telecommunications Act 1987, is a common carrier such as Telecom, Clear, and Bellsouth, not an ISP. The defence is one remove from ISPs which utilise telecommunications networks to provide connections but have no editorial control and act as conduits. Regardless of whether ISPs generate content or exercise minimal editorial control, the nature of the data volume and network connections make the imposition of strict liability unjust. An ISP can neither screen all (nor even a significant portion of) content provided by clients let alone the vast resources which users may seamlessly access from international sources. Nor are they legally capable of effecting such monitoring as, by virtue of section 216B of the Crimes Act, the use of listening devices is prohibited.[27] Under Clause 6, by virtue of such enveloping words as "transmit" and "communicate", a criminal offence would be committed by an ISP upon the passing of data constituting an objectionable image or sound through their service.

The formulation of a defence for network operators has itself been criticised on the basis that a defence necessarily entails submission to the criminal process. Network operators argue that the expense and stigma of having to provide evidence establishing a defence under the Bill is too onerous. The suggested alternative is to exempt network operators completely under clause 9 of the Bill and therefore cement the impunity of mere conduits. The future convergence of the telecommunications industry and the provision of multifarious services by current network operators may blur the categorisation of entities.

---

27 Clause 14, which removes the prohibition in respect of a belief (on reasonable grounds) by the Police that an offence under clause 6 or 7 is being committed, is arguably ineffective as s216B constitutes a prohibition, not an empowering provision, see The New Zealand Law Society, Submission on the Technology and Crimes Reform Bill, August 1994, 5. John Edwards, an information and privacy lawyer, has commented that the Police may not need a warrant to intercept e-mail communications, an area governed by the Privacy Act principles and s6 of the Telecommunications Act 1987: R Hosking "Police Need No Warrant to Tap Email, Says Top Lawyer" (1996) Computerworld 3.

The focus should arguably be on the potential and actual control exercised by an entity over content and dissemination of information.

The potential criminal liability faced by Internet users under the Bill is similarly threatening. Clause 6 imposes strict liability on any person who receives objectionable material through a telecommunications network. The strict offence of possession under section 131 of the FVPCA requires, as conventionally defined at common law,[28] at least some intention to exercise power and control over the object. Section 131 would therefore potentially exclude, as argued above, a user who merely browses the Internet. Clause 6 of the Bill imposes considerably broader liability and would arguably extend to the mere downloading of information, the content of which a user may have limited or no knowledge. Arguably, "receive" could be read, in line with the canon of interpretation that criminal statutes should be construed narrowly, as implying a conscious act of acceptance. This could take either of two forms; exclude merely unsolicited information from liability, or additionally, the unintended content of requested information. Extension to the latter interpretation is arguably not warranted on either semantic or practical grounds.

The above analysis has focused on the application of the Bill's offence provisions abstracted from the classification process. Clauses 3 and 13 of the Bill expressly adopt definitions and incorporate sections of the FVPCA. The classification regime imposed by the Bill does not, however, parallel that governing tangible publications. Clause 8 provides that:

> A person may be convicted of an offence under section 6 or section 7 of this Act if the image, sound, or live show is in all the circumstances objectionable, notwithstanding that it is a part only of an image, sound, or live show that is not objectionable.

The clause is subject to an internal tension between an assessment in "all the circumstances" that an image or sound is objectionable and the discretion to ignore the work as a whole. Section 3(4) of the FVPCA states that in defining a publication as objectionable the Classification Office shall consider:

> (a) The dominant effect of the publication as a whole:
>
> (b) The impact of the medium in which the publication is presented:...

Clause 3 of the Bill expressly adopts the definition of objectionable under section 3 of the FVPCA. The specific nature of clause 8 clearly overrides the application of section 3(4)(a) of the FVPCA. The result is an anomaly between the regulation of tangible and

---

28 See *R v Cugullere* [1961] 1 WLR 858.

intangible media, for which there is no clear policy justification.[29] The nature of digital multi-media is such that the separation of a discrete sound or image from a complete work could lead to substantial bias and imbalance in its classification.

The incongruous relationship between the FVPCA and the Bill is compounded by the provisions of clause 12. Whereas in relation to live shows the categorisation of publications parallels that of the FVPCA, the provisions concerning images and sounds are in stark contrast. Section 23(2) of the FVPCA allows a publication to be classified as objectionable except if restricted on the grounds of age, class of persons, or use for specified purposes, and is restated in relation to live shows in Clause 12(4) of the Bill. Clause 12(3) provides that the Classification Office, after considering matters referred to in section 3 of the FVPCA, shall classify the image or sound as either unrestricted or objectionable. The omission of the specified exceptions from objectionable classification in clause 12(3) imposes an absolute demarcation between unrestricted circulation and complete censorship. The consequences of such absolutes must be the enlarging of either category to subsume the retrenched area. The probable conclusion, considering that the omitted restrictions are exceptions from objectionable status, would be the entrenchment of a low threshold of objectionability which would be directed at the lowest common denominator, namely children.

In the alternative, if the exceptions to objectionable classification set out in section 23(2) of the FVPCA were adopted in relation to images and sounds, the nature of the Internet would make practical enforcement unachievable. The routing capability of the Internet, combined with the possible anonymity of both source and receiver, bar the confinement of images or sounds to particular persons or classes of persons or for particular purposes. Similar considerations apply to clause 12(5) of the Bill which empowers the classification of publications which would otherwise be objectionable, as restricted in order to be made available for "educational, professional, scientific, literary, artistic, or technical purposes".

Part II of the Bill is directed at providing additional penalties for those convicted of an offence involving the use of a telephone to "transmit objectionable material" and to "require a network operator to prohibit telecommunication with foreign telecommunication services

---

29 While the FVPCA does not always require an assessment of the work as a whole (section 3(2)), the TCR Bill completely removes the potential for such an assessment. For an extensive interpretation of section 3 of the FVPCA see New Truth & TV Extra, 4 November 1994, Unreported, June 1996, Film and Literature Board of Review, Decision 3/96.

whose programmes contain objectionable images or objectionable sounds". The definition of "programme" is that provided by section 2 of the Broadcasting Act 1989:

> Programme
>
> (a) Means sounds or visual images, or a combination of sounds and visual images, intended
>
> (i) To inform, enlighten, or entertain; or
>
> (ii) To promote the interests of any person; or
>
> (iii) To promote any product or service; but
>
> (b) Does not include visual images, whether or not combined with sounds, that consist predominantly of alphanumeric text.

The definition, which encompasses sounds and visual images, corresponds with the nature of an objectionable image or objectionable sound in clause 6 of the Bill. The qualifications contained in subparagraphs (i), (ii), and (iii) would, given the broad nature of such words as "inform, enlighten, or entertain", include most digital media. However, the proviso contained in (d) excludes media which consists principally of text. While this does not affect media with arguably the greatest potential impact and influence it does exclude a significant portion of Internet traffic.[30]

The cardinal misnomer in Part II of the Bill is arguably the requirement, in clause 18, of prohibiting telecommunication with foreign services where, "...any image or sound which forms part of any foreign telecommunications service [is]...objectionable".[31] The ability of network operators to comply with such a prohibition is constrained by both contractual and technical limitations.[32] In addition, blocking access to a foreign service would

---

30 For a more detailed discussion in the Canadian context, concerning virtually identical provisions, see D Shap "Hate Crimes in the Electronic Media" (1994) http://catalaw.com/logic/docs/ds-hate.htm.

31 Clause 21 defines a foreign telecommunications service as "...a person providing a service which consists wholly or mainly in the telecommunication from a place outside New Zealand of programmes which are capable of being received by a network in New Zealand". The isolation of a singular image or sound, as argued above, could lead to substantial bias as large proprietary networks which contain a wealth of information may be judged on the basis of a single transmission.

32 Telecom routes overseas calls to international gateways which interpret the initial digits of the telephone number and forward the call appropriately to international networks such as British Telecom and AT&T (beyond the jurisdiction of New Zealand's domestic legislation), see Telecom, Submission on the Technology and Crimes Reform Bill, August 1994, paras 4.5-4.9; Bellsouth is a signatory to the GSM Memorandum of Understanding which contractually obliges it to allow customers of other GSM networks to roam in New Zealand, see Bellsouth New Zealand, Submission on the Technology and Crimes Reform Bill, August 1994, 3.

necessarily involve obstructing transmission at an intermediate node, a regressive proscription which can be readily circumvented.[33] Such impediments have forced the proposed deletion of clauses 18, 19 and 20 by the Select Committee in favour of developing alternatives which focus on domestic providers and users.

Amendments proffered include broadening clause 10(4) to provide a defence where a bulletin board operator or service provider contracts with users on the basis that the user assumes full liability for any material which would be objectionable under New Zealand law. The avoidance of criminal liability through contractual relations is precluded at common law and there are similar policy arguments against its manifestation in statutory provisions.[34] Further, the potential for a standard form Internet contract raises questions as to the possible content and variation of terms.[35]

The most significant amendment proposed at the select committee stage was the imposition of a requirement that any person who owns or uses a computer accessible to children under the age of 16 with an international network link be obliged to install and maintain a security software program.[36] The proposition, while rightly focusing on the obligations of users, is uncertain in its scope and effect. Problems surround the definition of "accessible"[37] and the extension of the requirement to users of the computer as well as the proprietor.

D Bill of Rights Act 1990

Section 14 of the New Zealand Bill of Rights Act 1990 states that "[e]veryone has the right to freedom of expression, including the freedom to seek, receive, and impart information and opinions of any kind in any form". Clause 6, in providing for a complete ban on communication of objectionable material, prima facie is inconsistent with such a right. The Report of the Attorney-General, made under section 7 of the Bill of Rights Act and tabled in the House of Representatives,[38] attests to the inconsistencies of clauses 6, 7, 14(2) and

---

33 Users may simply establish access with foreign providers or use various international call back features. The prohibition is regressive in that successive services, assuming detection, would likely be prohibited until the eventual isolation of the local network.

34 See The New Zealand Law Society, Submission on the Technology and Crimes Reform Bill, July 1996, 2.

35 See MA Lemley "Shrinkwraps in Cyberspace" (1995) 35 Jurimetrics J 311.

36 Suitable security programs would be determined by the Classification Office and an appropriate offence provision (not having such a program installed and operational) created.

37 It is unclear whether the term contemplates access under normal circumstances or extends to unauthorised access, see above n 34, 3.

38 NZPD, vol 542, 3028, 24 August 1994.

29(4);[39] notwithstanding the potential for justified limitations and preferred interpretation under sections 5 and 6 of the Bill of Rights Act.

Overall, the failure of the TCR Bill is its inability "to recognise the practical realities of value-added network operation in a modern communications and multi-media environment".[40] The Bill attempts to impose an existing classification framework in a simplistic manner by attaching liability to entities, such as network operators and ISPs, without consideration for their functions and limitations. Trevor Rogers, MP, has commented that the scheme will be triggered by complaints and that prosecutorial discretion will ensure that criminal provisions are not enforced in an oppressive manner.[41] While the offence to the rule of law such a proposal presents must be noted,[42] a complaints based system is arguably circular in that it duplicates essential provisions of the FVPCA.

III THE COMMUNICATIONS DECENCY ACT 1996

In enacting Title V, known as the Communications Decency Act (CDA) 1996, of the Telecommunications Act 1996, the American Congress expressly acknowledged that the Internet represents "an extraordinary advance in the availability of educational and informational resources to our citizens" and accordingly maintained:[43]

> [i]t is the policy of the United States...to promote the continued development of the Internet and other interactive computer services; [and] to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation.

---

39 Clauses 6 and 7 were reported to be apparently inconsistent with section 14 of the Bill of Rights Act; clause 14(2) was deemed to breach section 21 (the right to be secure against unreasonable search and seizure); and clause 29(4) was assumed to be in breach of section 25C (right to be presumed innocent until proven guilty), see above n 38.

40 The Executive Committee of the Tuia Society and Information Technology Services VUW, Submission on the Technology and Crimes Reform Bill, July 1994, 1.

41 Commerce Select Committee Hearing on Technology and Crimes Reform Bill, 31 July 1996.

42 See, for a detailed exposition of what the "rule of law" encompasses, PA Joseph *Constitutional and Administative Law in New Zealand* (The Law Book Company Ltd, Sydney, 1993) 167.

43 Section 509 of the Communications Decency Act 1996.

A ACLU v Reno[44]

A conglomerate of plaintiffs[45] applied in the District Court for the Eastern District of Pennsylvania for a preliminary injunction to enjoin the enforcement of provisions challenged on constitutional grounds as infringing the rights protected by the First Amendment and the Due Process Clause of the Fifth Amendment. The challenges to section 223(a)(1)(B) (the indecency provision) and section 223(d)(1) (the patently offensive provision)[46] did not concern obscenity or child pornography, proscribed prior to the enactment of the CDA,[47] but the vagueness and overbreadth of the criminal provisions.[48] The central provisions of section 223 are as follows:

> (a) Whoever -
>
> (1) in interstate or foreign communications-...
>
> ...
>
> (B) by means of a telecommunications device knowingly-
>
> (i) makes, creates, or solicits, and
>
> (ii) initiates the transmission of, any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent knowing that the recipient of the communication is under 18 years of age regard less of whether the maker of such communication placed the call or initiated the communication.
>
> ...
>
> (d) Whoever -
>
> (1) in interstate or foreign communications knowingly-

---

44 *American Civil Liberties Union v Reno* 929 F Supp 824 (1996).

45 The plaintiffs, led by the ACLU, were many and diverse, ranging from civil liberty organisations to large corporate entities.

46 "Indecent" and "patently offensive" are used interchangeably in the court's decision as any distinction, although arguably justified by statutory interpretation, was not crucial to the plaintiffs claim; see above n 44, 850.

47 See 18 USC ss1464-65 (criminalizing obscene material) and 18 USC ss2251-52 (criminalizing child pornography).

48 The challenges also indirectly encompassed s223(a)(2) and s223(d)(2) which make it an offence to "knowingly permit" any telecommunications facility under a persons control to be used for the proscribed conduct in s223(a)(1) and s223(d)(1).

(A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or

(B) uses any interactive computer service to display in a manner available to a person under 18 years of age, any comment, request suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication...

...

(e)(5) It is a defence to a prosecution under subsection (a) or (d) that a person-

(A) has taken in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication specified in such subsections, which may involve any appropriate measures to restrict minors from such communications, including any method which is feasible under available technology; or

(B) has restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number.

The presumptive invalidity of content-based regulation led the court to apply a "strict scrutiny standard of review"[49] which would uphold the CDA only if "justified by a compelling government interest and...narrowly tailored to effectuate that interest".[50] The court made extensive findings of facts which necessarily influence and pervade the legal conclusions reached. Internet communications were approximately delineated into several categories:[51]

(1) one-to-one messaging (such as "e-mail"),

(2) one-to-many messaging (such as 'listserv"),

(3) distributed message databases (such as "USENET newsgroups"),

(4) real time communication (such as "Internet Relay Chat"),

---

49 The less than strict standard applied in *FCC v Pacifica Foundation* 438 US 726 (1978) and other broadcasting cases, as argued by the defendants, was therefore inapplicable.

50 Above n 44, 851.

51 Above n 44, 834.

(5) real time remote computer utilisation (such as "telnet"), and

(6) remote information retrieval (such as "ftp," "gopher," and the "World Wide Web").

The court emphasised that "receipt of information on the Internet requires a series of affirmative steps"[52] and that the ubiquitous anonymity of users made it "...either technologically impossible or economically prohibitive for many of the plaintiffs to comply with the CDA without seriously impeding their...constitutional right[s]".[53]

The court was unanimous in "inexorably"[54] upholding the plaintiffs claim that the relevant provisions were overbroad in reaching speech which is protected under the First Amendment. The reliance on third party co-operation (not enforced by the statute), purely hypothetical technical suppositions, and the resultant burden placed on a myriad of content providers, necessitated the conclusion that the statutory defences provided by section 223(e)(5) were inapplicable.

The majority,[55] while recognising such considerations entrenched on other areas, upheld the plaintiffs contention that the CDA was unconstitutionally vague. Buckwalter J, after noting that previous cases defined indecency with reference to contemporary community standards for the particular medium under consideration, held that the CDA encapsulated no such limitation but instead embodied a conflict between an apparent intention to impose a national standard and the prosecutorial requirement of a fluctuating community standard. Accordingly, he found "indecent [to be] unconstitutionally vague, and...the terms in context and patently offensive also so vague as to violate the First and Fifth Amendments".[56]

Dalzell J, dissenting as to constitutional vagueness, favoured a "medium-specific approach to mass communication [which] examines the underlying technology of the communication to find the proper fit between First Amendment values and competing interests".[57] Dalzell J held that "the Internet deserves the broadest possible protection from government-imposed, content-based regulation",[58] which manifested in the denial that Congress may regulate indecency on the Internet, a prospect the majority expressly left open.

---

52 Above n 44, 845.

53 Above n 44, 854.

54 Above n 44, 855.

55 Sloviter CJ and Buckwalter J.

56 Above n 44, 858.

57 Above n 44, 873.

58 Above n 44, 881.

The much maligned marketplace theory of First Amendment jurisprudence,[59] emphasising the low barriers to entry and the relative parity of speakers, underscored such conclusions which Dalzell J viewed as following inescapably from the findings of fact.

The court, implicitly highlighting the apparent redundancy of the legislation, was emphatic in maintaining that the conclusion of facial unconstitutionality did not expose minors:[60]

> Vigorous enforcement of current...laws should suffice to address the problem the government identified in court and which concerned Congress...the Justice Department itself communicated its view that [the CDA] was not necessary because it was prosecuting online obscenity, child pornography and child solicitation under existing laws, and would continue to do so.

The applicability of current obscenity legislation, and the rejection of a fundamental tangible/intangible distinction, is evidenced by *United States v Thomas*,[61] in which a criminal provision[62] which proscribed the transportation of obscene material was purposively interpreted so as to encompass downloading from an adult Bulletin Board Service.[63]

B Shea v Reno[64]

Shea v Reno concerned a more limited challenge of facial unconstitutionality toward the CDA. Joseph Shea,[65] who refused to join the ACLU lead coalition, sought a preliminary injunction on behalf of the American Reporter to restrain the Department of Justice from enforcing section 223(d) of the CDA. The District Court for the Southern District of New York, noting the contemporaneous nature of the *ACLU* decision,[66] declined to apply the doctrine of collateral estoppel, instead collating extensive findings of fact.

---

59 Above n 44, 879; the assumptions of such a theory (that the truth (or an ideal) is identifiable, preferable, and as such will prevail) are arguably rebutted by the "requirement" to censor the Internet, if the Internet is accepted as most closely achieving the free flow of information.

60 Above n 44, 856-857.

61 Unreported, 28 July 1994, WD Tenn, No. 94-20019-G.

62 18 USC s1465.

63 DD Burke "Cybersmut and the First Amendment: a Call for a New Obscenity Standard" (1996) 9 Harv JL & Tech 87, 118.

64 930 F Supp 916 (1996).

65 An editor, publisher, and part-owner of the American Reporter; a newspaper distributed solely by telecommunications.

66 *ACLU* was decided on 11 June, 1996; *Shea* was decided on 29 July, 1996.

The court recognised the same modes of access and communication concerning the Internet as were enunciated in *ACLU*, cognisant that such categories were dynamic with regard to the convergence of traditional media into "common forms of communication".[67] The court established that sexually explicit material did not constitute a significant portion of Internet content and further, that "...accidental retrieval of sexually explicit material is one manifestation of the larger phenomenon of irrelevant search results".[68]

Relying on the fact that previous challenges to indecency standards in relation to various communication mediums have been found unavailing by Courts of Appeals, the court, in findings directly contradictory to the majority in *ACLU*, denied the terms "indecent" and "patently offensive" and the contemporary community standards measure were unconstitutionally vague. The court held that liability for contravention of indecency restrictions has not been bound to the ability of content providers to monitor and assess contemporary community standards for a particular medium.[69]

Contrary to such conclusions, it can be argued that traditional Supreme Court jurisprudence has been informed by outmoded assumptions of geographical and sociocultural homogeneity.[70] Arguably, the traditional burden placed on content providers impliedly rests on the predominance of commercial providers and the ability to geographically restrict distribution in such mediums, an issue which the court refused to conclusively decide.[71]

The tension between analogy and selection of established legal doctrine, and developing reactive jurisprudence,[72] is evident in the consideration of contemporary community standards measures. The possibility of forum shopping by prosecutors and the reduction of content to the standard of the lowest common denominator, underpin arguments advocating a return to national standards and the conceptualisation of the Internet as a virtual

---

67 Above n 64.

68 Above n 44, 844; *Shea* determined that approximately 0.02% of all unique WWW sites contained sexually explicit material, above n 63, 931.

69 In fact, the court argued the Internet may provide an easier means to assess the relevant standard, above n 64, 937.

70 Above n 63.

71 The court considered the issue one of overbreadth, but declined, in light of other conclusions reached, to assess whether any such overbreadth was substantial, above n 64, 938.

72 See RS Zembek "Jurisdiction and the Internet: Fundamental Fairness in the Networked World of Cyberspace" (1996) 6 Alb LJ Sci & Tech 339; FH Cate "The First Amendment and the National Information Infrastructure" (1995) 30 Wake For LR 1.

community.[73] The inter-jurisdictional nature of Internet communications can arguably be accommodated by established doctrines of personal jurisdiction, operating within national and international law, embodying requirements of minimum contact and due process.[74] However, such doctrines reflect prescriptive rather than effective jurisdiction and have been formulated in more static, geographically restrictive environments.

The court in *Shea*, while not sympathetic to the above arguments, were unpersuaded as to the ability of content providers to avail themselves of the CDA's specified defences. The verification of the age of users, requiring the implementation of extensive databases and the sacrifice of anonymity, was deemed too "burdensome".[75] Further, the provision of a good faith defence, through screening, tagging and registering content,[76] was ruled technically infeasible:[77]

> [e]ven if it were established that the statute is to some limited extent effective in protecting minors from sexually explicit material on line, and that nothing short of a total ban on indecent communication could be as effective, it is not obvious that the benefits thus achieved would outweigh the burden...

Both courts emphasised that "[b]ecause of the rapidity of developments in this field, some of the technological facts we have found may become partially obsolete by the time of publication of these [f]indings".[78] The Internet cannot be defined and categorised as a

---

73 See FB Lim "Obscenity and Cyberspace: Community Standards in an On-line World" (1996) 20 Colum-VLA JL & Arts 291; the associated problems have also proved fertile ground for arguments addressed toward abolishing censorship altogether in favour of personal injury based torts, see above n 63.

74 See RS Zembek "Jurisdiction and the Internet: Fundamental Fairness in the Networked World of Cyberspace" (1996) 6 Alb LJ Sci. & Tech 339. Minnesota provides an example of a more robust approach: "Warning to all internet users and providers ...[p]ersons outside of Minnesota who transmit information via the internet knowing that information will be disseminated in Minnesota are subject to jurisdiction in Minnesota courts for violations of state criminal and civil laws", "Minnesota Attorney-General Warning" http://www.state.mn.us/ebranch/ag/memo.txt.

75 Association with "adult" verification services or the utilisation of CGI (common gateway interface) scripts, costing approximately US$1 per transaction, were ruled economically prohibitive, above n 64, 934.

76 The court considered PICS and other tagging schemes and registration of sexually explicit content in relation to both server and client software, above n 64.

77 Above n 64, 941.

78 Above n 64, 848. The Supreme Court has recently affirmed the decision of the District Court in *ACLU v Reno*. Stevens J, who delivered the opinion of the court, held that the CDA "... places an unacceptably heavy burden on protected speech, and that the defences do not constitute the sort of 'narrow tailoring' that will save an otherwise patently invalid unconstitutional

monolithic medium. The development of the Internet from its defence force origins represents the emerging possibilities to which such a multi-layered value-added network can be applied.[79] In delineating the prevailing features and technology which currently exist it must be remembered that the amorphous nature of the medium readily consigns such profiles to historical analysis.

The ineffective nature of the CDA, in only regulating domestic content providers,[80] underscores the findings in *ACLU* and *Shea*.[81] The courts, while not explicitly pronouncing on the sagacity of the legislation, were desirous of indicating that the statute actually advantaged extra-territorial content providers who could act with impunity.

IV OTHER REGULATORY MODELS

The territorial limitations of domestic legislation necessarily preclude the effectiveness of the above considered isolated attempts at regulation:[82]

> Regulation is not an issue for each individual service provider or user or even nation. The global nature of the network makes this a global problem and to be tackled effectively it must be tackled on a global scale.

Nevertheless, in developing domestic and international measures, the formulations adopted by other jurisdictions may provide instances of applicable legislative and regulatory models. The British Home Office and Internet Service Providers Association

---

provision". The court, in stating that the breadth of the CDA was "wholly unprecedented", acknowledged the Internet shared "no comparable history" including regulation and supervision, with other communication mediums. The court declined to consider the Fifth Amendment issue, instead relying on the overbreadth inquiry in regard to the First Amendment. The vagueness of the legislation, of particular concern due to the content based regulation and criminal penalties, imposed "an especially heavy burden" that the Government was unable to discharge. O'Connor J, with whom the Chief Justice joined, dissented in part, arguing that the CDA be sustained to the extent it does not substantially interfere with the First Amendment rights of adults. Although acknowledging the Internet remains largely "unzoned", O'Connor J's reasoning is predicated on the potential "transformation" of Cyberspace to approximate the physical world's characteristics of geography and identity. Http://www.aclu.org/court/renovacludec.html.

79 For a greater exposition on the origins and development of the Internet, see E Krol *The Whole Internet User's Guide* (Special Edition, O'Reilly & Associates, Inc, Sebastopol, 1994).

80 Thereby leaving up to 30% of sexually explicit content, generated outside the United States, unregulated, see above n 64, 940.

81 The court in *Shea* declined, based on its other conclusions, to rule on whether the statute's ineffectiveness would render it constitutionally defective, above n 64, 940.

82 S Weatherall "Internet Service Providers Association - Update" 4 IT Law Today, 1996, 5, 6.

have advanced a draft code of practice, founded on a "reasonable endeavours principle",[83] which recognises that an ISPs editorial control may vary considerably, and qualifies obligations accordingly.

The Australian federal classification scheme, implemented by the Classification (Publications, Films and Computer Games) Act 1995, represents a cooperative approach between the commonwealth, states and territories.[84] The establishment of classification guidelines under the legislation provides the foundation for classification codes in relation to television broadcasting and reflects an ethos of consistent classification across mediums, recognising that applicable methods may differ. The proposed extension of such a regime to online services, given the implementation of a "national strategy aimed at the adoption of new information and communications services and technologies",[85] as variously defined, is manifested in the constitution of several independent federal investigations.

The Bulletin Board Task Force,[86] which terms of reference were to examine and establish regulatory options for BBSs,[87] was criticised for addressing archaic ideals in its assumption of system administrators control over access and content.[88] The Task Force identified several regulatory schemes, ranging from the application of classification and offence provisions to the formulation and adoption of industry guidelines.[89]

The Information and Communications Services Policy Group, which issued a consultation paper on the regulation of on-line information services,[90] was subsequently directed to stimulate consultation on developing the above recommendations and their application to broader telecommunications capabilities.[91] The Australian Broadcasting Authority also issued a consultation paper in its investigation into the content of on-line

---

83 What is considered reasonable for an ISP to take responsibility for, or maintain control of, will depend on practical and technical limitations, see above n 82.

84 See "Consultation Paper on the Regulation of On-line Information Services" (July 1995) http://www.dca.gov.au/pubs/paper_2.html.

85 Above n 84.

86 Established by the Minister for Communications and the Arts, and the Attorney-General in November 1993; and reported on 5 October 1994, see above n 84.

87 See above n 84.

88 A criticism which can be made of the TCR Bill; see Australian Computer Society "Submission on the Regulation of Bulletin Board Systems" http://www.efa.org.au/Issues/Regulate/.

89 See above n 84.

90 Published 7 July 1995, see above n 84.

91 This can be accredited to the substantial decline in closed, proprietary BBSs, see above n 88.

services and the appropriateness of developing a code of practice.[92] In recognising that a technologically specific approach to the issue would be redundant, both bodies focussed on the application of existing classification standards to Internet content. The papers contemplate industry self-regulation and the establishment of a complaints review system coupled with a national education strategy. The problems associated with liability of access providers storing or transmitting content without knowledge or intent and the enforcement of offence provisions are addressed through the recommendation of defences where providers take reasonable steps to control content or reasonably believe content not to be objectionable or restricted.[93]

The above approach, while admitting certain technical limitations, persists in the pursuit of legislative and regulatory control over easily identified entities. The adoption of a code of practice, while allowing more dynamic and reflective change in line with technological advances,[94] continues to concentrate on subjecting access providers to offence provisions with limited and infeasible defences.[95]

The admission that "no single national body can have effective control over the content and regulation of on-line services available in a particular country"[96] has not dissuaded the enactment of state and territorial legislation based on the above recommendations. The Classification (Publications, Films and Computer Games) (Enforcement) Act 1995 (Victoria) and the Censorship Act 1995 (Western Australia) embody the above characterisation of universal offence provisions subject to arguably innocuous defences. New South Wales has rejected draft legislation, parallel to those above, in order to establish an industry code of practice as developed by the Australian Broadcasting Authority.[97]

V CONCLUSION

Although media have acquired the functions of the press, they have not yet obtained the rights of the press. The rate of technological change has outstripped the ability of the law, lurching from one precedent to another, to address new realities. Novel communications are

---

92 The authority's reporting date was set at 30 June 1996.

93 See above n 84.

94 An independent complaints review system would also address administrative justice issues between providers and users, a subject beyond the scope of this article.

95 Similar criticisms to those made in *ACLU* and *Shea* can be made in regard to subjecting providers to the expense and stigma of raising a defence in a criminal trial, and that the reasonable steps defence cannot be claimed if no reasonable or feasible content restrictions exist.

96 "Issues Paper on the Investigation into the Content of On-Line Services" (Dec 1995) http://www.dca.gov.au/aba/hpcov.htm.

97 See "Censor's hands off the Internet" Australian Financial Review, Australia, July 12, 1996, 55.

pressed into service while still in their infancy, and the legal system's initial encounters with these newborns have a lasting influence.[98]

The legal fascination with precedent and analogy may appear opposed to the development of a reflective and informed jurisprudence concerning emerging technologies. However, such reasoning may, if tempered by the realities of modern telecommunications, imbue the judicial and regulatory approach to technological advancements with an awareness of the necessarily resulting societal change.[99]

The interconnected nature of the current Internet, replete with redundant routes, requires that the interception of information, to be effective, must occur at either the source or destination. Censorship at an intermediary node can be freely circumvented and the immense volume of information generated daily, together with private encryption techniques,[100] preclude effectual monitoring. As the point of dissemination, at least for New Zealand and most countries outside the United States, is primarily extra-territorial the realisation is that "we can meet diverse needs by controlling reception rather than distribution".[101]

"Governments will need to take pro-active stances in instructing rather than legislating".[102] The current censorship laws in New Zealand, although potentially draconian, are capable of prosecuting instances of abuse and prohibiting the storage or recording of objectionable material on computer hardware. Legislation, if applicable at all,[103] cannot focus on the common carriers which operate the networks and provide connection to the Internet, and must be sufficiently flexible to accommodate the increasing technological convergence of traditional media.

---

98 RF Goldman "Put another Log on the Fire, there's a Chill on the Internet: the effect of Applying Current Anti-obscenity laws to Online Communications" (1995) 29 Geo L Rev 1075, 1075.

99 Hass argues that technological revolutions have highlighted the nature of the current received moral tradition that is our rightful inheritance but which has been almost irretrievably lost, see J Haas "Thinking Ethically about Technology" http://www.ee.gannon.edu/~frezza/papers/Johnhaas.

100 Encryption software is freely available on the Intenet, see Bellsouth New Zealand, Submission on the Technology and Crimes Reform Bill, August 1994.

101 Council of the Internet Society of New Zealand Inc, Submission on the Technology and Crimes Reform Bill, July 1996, 4.

102 Above n 2.

103 For a critical assessment of legislative models in relation to the Internet, see J Kay "Sexuality, Live without a Net: Regulating Obscenity and Indecency on the Global Network" (1995) 4 S Cal Interdisciplinary LJ 355.

The development and adoption of codes of conduct for Internet providers, in establishing required complaints procedures and industry standards, cannot exist as an isolated measure but must be coupled with education and inculcation of user responsibility. Technological developments, such as the recent evolution of screening software,[104] should be encouraged, and the co-operation of nations, with a view to establishing feasible solutions, instituted and maintained.

---

104 See above n 79.