FOREWORD

I am pleased to introduce Dr Judit Bayer's research on the topic of Internet Service Provider ("ISP") liability. Dr Judit Bayer was appointed New Zealand's first InternetNZ Senior Research Fellow in Cyberlaw at Victoria University of Wellington, Faculty of Law, in 2006.

InternetNZ, the not-for-profit organisation that fosters co-ordinated and co-operative development of the Internet in New Zealand, sponsors the fellowship in Cyberlaw. The fellow is based at the Faculty of Law, Victoria University of Wellington. The main aim of this "joint-venture" fellowship between Internet NZ and the university is to produce research on internet and telecommunications-related legal subjects to enhance New Zealand's understanding of legal issues as they relate to technology.

InternetNZ proactively encourages debate and development of public policy in an open and transparent environment and believes this fellowship project adds significant value to the decision making process.

Dr Bayer's research considers ISP liability within a variety of different fields of New Zealand law including defamation, copyright, hate speech and related freedom of expression issues. She draws on overseas experience of ISP liability schemes and evaluates the pros and cons of those schemes. The research concludes with a practical proposal for New Zealand. Her conclusions reflect a balance of competing interests and the best fit for the policy that underlies the areas of law where ISPs may find themselves liable. Dr Bayer not only discusses the balance of interests, but shows in diagrammatic form the relationship between the interests at stake. I am particularly delighted with the proposal's graphic representations of the significance of competing interests relative to each other.

For readers with time to absorb all of the research there is much detail assimilated conveniently in these pages. For those with less reading time the concluding proposal is a valuable summary that merits "stand-alone" reading.

This paper was completed and accepted for publication in May 2007.

Susy Frankel

Professor of Law

LIABILITY OF INTERNET SERVICE PROVIDERS FOR THIRD PARTY CONTENT

Judit Bayer*

I INTRODUCTION

A The Main Function of ISPs

This research focuses on the legal status of internet service providers. Operating the network that is commonly called the internet requires the cooperation of several different intermediary actors. Internet service providers (ISPs) play a crucial role in this process. They provide access to the World Wide Web, and allow users to store and publish content. Finally, one could say that ISPs establish the connection between people and content on the internet. They connect people with the physical network, which makes them "the most important and obvious focal point of Internet control".[1]

ISPs provide not only one type of service, but a multitude of services. For practical reasons, I focus on the four most basic activities. The first and perhaps most essential activity is providing access to the internet for users. This creates the fundamental connection between a person and the internet, allowing them to both download and upload any content. The second most characteristic service is providing hosting services for providers of content. This is one step beyond providing access only, because by this an ISP accommodates its server to the subscriber not only for temporary traffic, but for a more or less constant storage of their personal content. While the first service could be compared to the telephone service, the second is unique in its nature. Most often it has been compared to the distributors' activity.[2] This service raises the most legal issues, although

---

* Dr Judth Bayer, Internet NZ Senior Research Fellow in Cyberlaw, based at Victoria University of Wellington 2006. I would like to express my special thanks to those colleagues who have helped my work. Among them I am especially thankful to Susy Frankel, Dean Knight, Ian Macduff, Nicole Moreham, Steven Price, Katrine Evans, Lindy Siegert, Judge David Harvey, and the all members of Internet NZ.

1 Jack Goldsmith and Timothy Wu "Digital Borders – National Boundaries Have Survived in the Virtual World – and Allowed National Laws to Exert Control over the Internet" [2006] Legal Aff 40, 6.

2 Ronald J Mann & Jane K Winn "Electronic Commerce" Aspen Law New York 2002 114. See also *Zeran v America Online, Inc* (1997) 958 F Supp 1124 (ED Va) *[Zeran No 1];* (1997) 129 F 3d 327 (4th Cir) *[Zeran*

not the most complicated ones. Discussing the legal implications of this will form a major part of this study.

The third type of service is caching the transferred content. This means automatically creating a temporary copy of the material, so that it can be accessed more easily and quickly the next time when it is needed. When a page consists of several details, such as a news site, usually not all details change regularly. Only some content parts change on a daily basis, but the frame, the name and logo of the publisher and other parts are usually constant. The cache copy enables the requesting machine to access the page from the closest possible exemplar – the cache – and to reload only those details that have changed.

ISPs do not know the content of the cache, nor do they know the content of the hosted material. However, there are cases when ISPs intentionally create cache copies of selected content. The purpose is to help easy access to that certain content, when a high number of requests can be expected. They follow the same logic as hydroelectric power plants: the highest performance is needed in peak hours when the vast majority of people get up in the morning, bathe, and leave for work, and when they arrive home again in the evening. This clearly has practical benefits, but it is different from the original sense of "cache" and this difference may be important from a legal aspect. This becomes significant when analysing the liability of ISPs. In the latter case, it selected certain content and intentionally decided to create a copy of it, which is very different from an automatic, technical action, the original form of cache. In some cases the ISP need not be aware of the content, only the fact that more than an average number of people want to access it. Being aware of this fact, ISPs may find it useful to make a copy, thereby decreasing their costs of transmission. But, at least in some cases, the situation is different: knowing the content actually allows the ISP to precalculate that an above average number of users will want to have access to it.

Finally, the fourth activity of ISPs is providing searching services. I list them as less typical, because not all of the ISPs perform this function. Searching tools are indispensable in the use of the internet. It is essential that there are several search engines so as to maintain variety and competition. Providing searching services may also occasionally attract lawsuits, because the ISP can be regarded as providing tools for access to an illegal site.[3] Search engines also appear to be a battlefield between competitors under the DMCA in the United States.[4] Users can get information

---

No 2]; *Blumenthal v Drudge and AOL, Inc* (1998) 992 F Supp 44; *Cubby Inc v Compuserve Inc* (1991) 776 F Supp 135; *Stratton Oakmont Inc v Prodigy Services Co* (1995) 23 Media L Rep 1794 (NY).

3 See also Glenn Chapman "Porn link case testing web freedom" (2006) Australian IT.

4 Electronic Frontier Foundation (EFF) "Briefing Paper: Internet Service Provider Safe Harbors And Expedited Subpoena Process in the US Digital Millenium Copyright Act and Recent Bilateral and Freetrade Agreements" (7 June 2005) 5; Jennifer M Urban and Laura Quilter "Efficient Process or Chilling Effect? Takedown Notices under section 512 of the Digital Millenium Copyrigh Act" (2006) 22 Santa Clara Computer & High Tech L J 621, 654.

about materials available online only through search engines. Therefore search engines are able to influence the users' perception about reality. It is a real threat that search engines discriminate between various content pages upon criteria that are not influenced by the user. It should be considered whether search engines perform public service functions and accordingly have responsibilities to maintain their neutrality.

We can find further differences between the various types of services. For example, providing access and hosting happen mainly on the basis of a contract, whereas caching and searching do not. However, there are some exceptions: by hosting bulletin boards or chat rooms, ISPs do not enter into a contract with each of the participants. On the contrary, most of these participants are anonymous and they use the services just as spontaneously as searching services.

ISPs usually perform multiple functions. An average ISP would provide at least three of the above mentioned services, as well as provide its own content – at least when it advertises its own product and maintains its own website. Many ISPs provide a large amount of other content for business purposes (for example AOL), whereas a content provider can provide hosting services when it has a bulletin board and lets other users publish postings on it. Further, many companies have their own servers where they store their own content. However, they still have to buy internet access from an ISP.

Originally, one of the main activities of ISPs was to host Usenet/newsgroups and bulletin boards. These services that are still popular can be compared to today's internet forums, the difference being that they were not parts of a content site, but were hosted by the ISPs themselves. Usenet was hosted by multiple ISPs at the same time and the requesting machine could download content from the closest server.[5] Some of the first court cases that started because of illegal online content and which affected ISPs were caused by Usenet or newsgroups postings.

B Second-layer Service Providers

As internet content becomes more varied, it is impossible to ignore that many content providers provide additional services for other users. Blogging sites invite users to provide content through their blog-templates. Blogs invite comments, creating a third level of content. Many content providers, including newspapers and governmental departments operate a forum where their readers can submit comments. YouTube enables uploading of videos by any ordinary user.

These content providers mediate another person's content. They have the technical capacity to monitor content, but often the sheer volume of material provided by others exceeds their capacity to do so. The main activity of these services is to enable others to publish their own content. Unlike a newspaper editorial office, which welcomes articles and reviews them and edits them individually before publishing, these sites only transmit the content that their "clients" have submitted.

---

5 The Usenet archive was bought by Google in 2005.

Controlling and editing the content would be contrary to the original idea and probably decrease the popularity of such sites. Even if they exercise some sort of control, there would be a delay between publication and moderation.

The liability of such service providers is entirely unclear. They are not service providers in the original sense of the word, because they themselves provide content, and do not provide basic services. A blogsite (for example: www.blogger.com) acts as a service provider in relation to the individual blogger, whereas the blogger acts as a service provider in relation to those users who provide comments. Saying that they are liable for moderating such content would mean that it is illegal to leave a blog unattended.

I call these actors second-layer service providers. The scope of these may expand in the future: "blogging is clearly the next frontier in this intersection of Internet and First Amendment law" writes Machado.[6] Their liability might be different from ISPs in general, but the role they fulfil is in many aspects very similar. Some forms of this content are discussed in more detail below under E(3).

II THE DIFFERENCE BETWEEN ISPS AND TRADITIONAL MEDIA ACTORS

When illegal content was encountered on the internet, the first reaction was to "accuse" ISPs. Traditionally, in print media it was the publisher, and in broadcasting it was the broadcaster, who was held liable. Therefore, at first the ISP seemed to be a logical culprit since it was the one who had technical control over the content. Particularly, the actual content provider was often anonymous, or it was difficult to reveal their identity. However, there is a fundamental difference between a publisher and an ISP. To explain the nature of this difference I analyse the nature of the medium.

For the purposes of this study, I will call radio, television and newspapers "traditional media". As I argue below, the internet differs in very important aspects from these.

A The Interactive Medium

Before the 1990s, media operated in the form of one-to-many communication. As a contrast to this, internet is a tool that facilitates many-to-many communication, and although there are many distinctive actors, there are millions of ordinary contributors too.

Already used by traditional media, the most popular programmes were the interactive ones which enabled people to participate. People enjoy being heard, and are keen to cooperate in the creation of programmes. Newspapers often run readers' columns; radio's most popular programmes have been phone-in programmes, and broadcasters build on talk-shows and reality-shows.

---

6 Leslie Paul Machado "Immunity under §230 of the Communications Decency Act of 1996: a Short Primer" (2006) 10 Journal of Internet Law 3, 8.

Contributors or "civil" participants of such programmes are not legally responsible for their own performance: the programme is edited by professional staff. The conversations are always guided or moderated and the programmes often are cut. In contrast, the internet gives everybody the opportunity to publish whatever they want to individually. There are no strict constraints of format, access, or even financial resources. The content submitted by these people is not guided, not moderated, not edited and not cut. People express themselves without the help of a mediator filtering their words.

This leads to the conclusion that the internet is not a content medium as it was understood during the 20th century. It is rather a new platform of communication which can host every known method of communication, whether it be written text, pictures, moving pictures or sound. It is also a tool for commercial activities for both consumers and businesses, of teaching and learning, and many other activities. When users engage in internet shopping they do not use "media" in the traditional sense of the word. More exactly, they use a "medium" in the original, Latin meaning of the word: they use a mediator for their actions. The earlier medium templates restricted what form and type of content the medium could transmit, the internet's technology does not.

The internet can be used to read a newspaper, listen to radio and watch television, thus as a traditional, one-to-many medium. But its "audience" can act not only as content recipients but also as content providers: sending emails, instant messages or making phone-calls. Beyond these forms of one-to-one communication, users can also set up their own websites, acting themselves as publishers and use it as a new type of one-to-many medium. Finally, when users enter into conversations in bulletin boards, internet forums, chat-rooms or blogs, they use the most revolutionary form of the internet: many-to-many communication.

To sum up, the internet embraces all aspects of media: newspaper, television, radio, telephone, letter, book, and so forth. Beyond the known forms of media communication it has introduced the new concept of many-to-many media. Sometimes the publication is performed by a professional publisher (for example: <www.nzherald.co.nz>), sometimes by a private person (for example: <www.kiwiblog.org.nz>).

B Spontaneous Content

Unlike traditional media, internet communication consists not only of edited programming by distinguishable companies. Ordinary users provide a significant amount of the material. The line between the audience and the publisher becomes blurred.

ISPs are intermediaries who are in a special situation. On the one hand, they are in control of the content technologically, but, on the other hand, they are not aware of the content, and are therefore unable to systematically exercise such control. Even if an ISP is aware of the content, it is often difficult to make a judgement as to its legality. They are just intermediaries and for that reason they should never be treated as publishers.

Like telephone companies, ISPs only provide the facilities and do not know what content is going through the wires. However, there are significant differences between telephone companies and ISPs. The internet needs a similar infrastructure to that of telephone, which is often – but not always – provided by telephone companies. The qualitative difference lies in the ISPs, who create nodes and thus make a global network. They could also be compared to telephone switchboard operators, but then there is a variety of platforms, and a possibility of storing, not only transmitting data.

III IN THE ABSENCE OF A SPECIFIC REGULATION

If a country does not have specific laws about the liability of ISPs, then their liability needs to be decided case by case upon the existing legal rules. The outcome will depend on how the courts interpret those rules. Since ISPs fulfil a role that had not previously existed, it is difficult to foresee the outcome. Under traditional liability structures they could easily be found liable for content provided by someone else.

While their duties are not clarified, they could be found negligent for not knowing that illegal content was imparted, if the court finds they should have known (for example if it could have been "constructed" from the domain name of a site hosted). Strict or absolute liability clauses pose a particular danger to ISPs since the mental element would not be required to be held liable. Therefore the main advantage of any regulation is the legal certainty that it would provide. Further, all such rules worldwide in one way or another limit the liability of ISPs. Unfortunately, even today ISPs have to struggle with lawsuits from time to time, being sued for content that they did not provide.[7]

If ISPs are exempted from liability, authorities or an aggrieved party will have a strong incentive to find the actual content provider in order to prosecute her or demand compensation for damages. To find the perpetrator, they would turn to the ISPs and demand personal data of their subscribers or their users. This raises another aspect of ISPs legal obligations: how far are they supposed to protect the privacy of their users? Sometimes the sole purpose of identification is to apply out-of-court counter measures against the user, rather than to pursue a lawsuit.[8] Some authors think, that if the defaming user is a disgruntled employee, it is right to use a subpoena to reveal their identity and apply employment-related consequences (dismissal). Others argue that the identity should only be revealed if the plaintiff can present a substantial claim.[9] ISPs could hold sensitive information about

---

7 See Michael Geist "Libel Case Key For Internet Free Speech" (2006) Toronto Star

8 Joshua R. Furman "Cybersmear or Cyber-Slapp: Analyzing Defamation Suits Against Online John Does as Strategic Lawsuits Against Public Participation" (2001) 25 Seattle U L Rev 213; *Raytheon Co v John Does 1-21* Civil Action No. 99-816 (Commonwealth of Massachusetts Superior Court, Middlesex County, Filed Feb 1 1999).

9 Konrad Lee "Anti-employer Blogging: Employee Breach of the Duty of Loyalty and the Procedure for Allowing Discovery of a Blogger's Identity Before Service of Process is Effected" [2006] Duke L & Tech

their users by tracking their browsing or searches. It is yet unsettled how much should be recorded and revealed in such the circumstances, and whether ISPs or plaintiffs should bear the costs of a court order.[10] It is outside the scope of this study to give a comprehensive analysis of these problems. However, where possible I will mention and later address the question of identification among the proposals.

IV GENERAL LEGAL QUESTIONS

A Issues Addressed in this Paper

Some of the most significant illegal activities that may be performed by clients or users of ISPs will be discussed below. These may have an effect on ISPs, unless it is clarified that they cannot be legally liable. It would be impossible to list and examine individually all activities that may cause harm or which qualify as an offence or a crime. Therefore I select some significant and typical examples. Below I also detail what will and will not be discussed in this study.

Harm caused by ISPs to their clients is outside the focus of this paper. These contractual obligations are not modified by the existence of the internet. ISPs are liable for expediently fulfilling their obligations and providing the service as agreed, just like any other company.

Liability for the content of advertisements will not form part of this study either. It is already settled in other media situations that a transmitter of advertisements is not liable for the content of the advertisement. In ancient Roman Law, if a hanging advertisement board fell down and caused harm or injury to someone, the advertiser was liable, rather than the owner of the building.

I will only deal with some of the most typical cases of illegal content, and use examples from both civil and criminal liability. Whatever the content, the question is: what is the extent of the duty an ISP owes for content carried, but not provided, by them? In my opinion the acceptable answer is "nothing". But some jurisdictions impose conditional obligations on ISPs.

The reform of the copyright law is currently in progress in New Zealand. This will be described below. The reform process is in line with the findings of this paper but no detailed provisions are known at this stage.

Where an ISP has a financial interest in providing a certain type of content, it may justly be made liable. This would mean that it gets more financial revenues from one type of content than from another. If an ISP starts to differentiate between content, its argument of being an innocent carrier becomes weaker. An example is seen in the Australian case of *UMA v Cooper*[11] where the

---

Rev 2; See also Michael S Vogel "Unmasking 'John Doe' Defendants: the Case Against Excessive Hand-wringing over Legal Standards" (2004) 83 Or L Rev 795.

10 See also *Totalise v The Motley Fool* [2002] 1 WLR 1233 (EWCA).

11 *Universal Music Australia Pty Ltd & Ors v Cooper & Ors* [2005] FCA 972 *[UMA v Cooper]*.

ISP provided hosting for free, and in terms of a barter agreement it placed its advertisement on the website. The website in question enabled music pirating and attracted a very high number of visitors. Thus, indirectly the ISP had an extra benefit from hosting illegal content, although it was not strictly speaking a financial benefit, but rather an advantage "arising from the display of the reference".[12]

The ISP was found responsible because it lost its defence of innocence. Although the respondents claimed that they did not know about the content of the site, the court, also considering other circumstances, did not accept their statement.[13]

> I do not accept that Bal and Takoushis were unaware of the contents of the site or that they failed to take any steps to inform themselves as to the volume of traffic that the website would be likely to attract.

The court held that because of the business decision that the ISP took, it is unlikely that they did not pay attention to the content that was hosted by them:[14]

> Moreover, it is in accordance with reasonable expectations as to the behaviour and experience of Bal in hosting as a commercial operator that he would have been keen to ensure that E-Talk/Com-Cen was receiving some benefit in return for hosting the website for free.

Should the ISP have hosted all websites for free in exchange of their advertisement, it could not have been proven that they took this decision. However, that would not have been a reasonable business decision, because: "[t]he provision of these hosting services was a significant source of the revenue for Com-Cen Internet Services".[15] Note that the ISP was liable not for benefiting from an illegal action, but this could serve as proof of their awareness of the page's content, which was illegal.[16]

The principle of exemption should be content neutrality, arising from the assumption that ISPs are not aware of and do not discriminate with respect to content. If an ISP knowingly breaches this principle, treating a site in any way differently from others, this could serve as a basis for liability.

Defamation is one of the most frequent causes of action in lawsuits relating to internet content; therefore I will often refer to defamation as a general example. It has perhaps the widest case law thus far. It is also a good example because the principles of defamation are very similar in different jurisdictions, even if the procedure is different.

---

12 *UMA v Cooper*, above n 11, 117 Tamberlin J.

13 Ibid, 119 Tamberlin J.

14 Ibid, 115 Tamberlin J.

15 Ibid.

16 See also Part III.

B What Amounts to Publication in an Online Environment?

At common law, publication for the purposes of defamation has taken place if the information has been disclosed to anyone other than the plaintiff. If the publication was made through newspaper, radio, or television, there is no need to prove that it was published to any specific person or persons.[17] It cannot be proven whether a defamatory TV programme in fact was watched by anyone. But the number of people accessing an internet site can be proven. There have been cases where the court accepted (or did not reject) the argument that there were so few hits on the website that the level of publicity may have been insignificant. In *Dow Jones v Jameel*[18] it was proven that the defamatory site had altogether five visitors in England – most of them probably members of the court and the plaintiff himself. In a second case, *Al Amoudi v Brisard and JCB Consulting*[19] the newspaper could show that there had been only a few hits from England but a large number of other hits from unidentified locations. The judge let the jury decide whether the publication was significant enough locally. A similar situation led to a similar decision in the Canadian case of *Bangoura v Washington Post*,[20] where the offline journal had seven subscribers only, and the online articles had only two hits, both by Mr. Bangoura's lawyer. Therefore, the court found that there were no damages in Canada. However, in all of these cases, both the defendants and the plaintiffs were only loosely connected to the United Kingdom or Canada, respectively. This was the main reason for rejecting jurisdiction, but these cases could open the door for others where the relevance of publication is regarded as an essential element for the purposes of defamation as well as jurisdiction. (One could conclude that a plaintiff who has been defamed through the internet, simply has to ensure enough clicks on the defaming page so as to produce the necessary number of hits.[21])

Of course, internet publication generally would amount to publication for defamation purposes.[22] But, when talking about "internet publication", it is still not defined who counts as a publisher.[23] Burrows does not conclude whether ISPs are publishers or not,[24] and the possibility cannot be excluded that ISPs may be treated as publishers. They may avail themselves of the defence of innocent dissemination in defamation cases, and in certain other cases lack of intention

---

17 Stephen Todd (ed) *The Law of Torts in New Zealand* (3 ed, Brookers, Wellington, 2001) 825.

18 *Dow Jones v Jameel* [2005] EWCA Civ 75.

19 *Amoudi v Brisard and JCB Consulting* [2006] EWHC 1062 (QB).

20 *Bangoura v Washington Post* 2005 Carswell Ont 4343.

21 See also "Count the Readers Before Suing For Internet Libel" (15 June 2006) OUT-LAW News.

22 Todd, above n 17, 826.

23 The place of publication has been more often the centre of the dispute, as in the cases above and also in *Dow Jones & Company, In. v Gutnick* [2002] HCA 56.

24 Todd, above n 17.

could be a defence. By this, a similar result is achieved to the notice-and-takedown system of the various other jurisdictions, where ISPs are not liable for content, unless they knew or had reason to know that the content was illegal. The difference, however, is in the burden of the proof: in notice-and-takedown systems ISPs are not liable until it is proven by the appellant that they knew about the content, whereas in New Zealand (for example in defamation law) it is the ISP who has to prove that they were innocent disseminators.[25]

Exempting ISPs from liability is not the same as exempting the actual provider of illegal content. On the contrary: it creates a more secure environment where plaintiff, ISP and the authorities may focus on actually finding the real perpetrator and punishing her, rather than making a culprit of the "messenger".

C Some Typical Forms of Internet Publication

1 Newsgroups, forums, usenet and chatrooms

These belong to the most specific examples of internet communication, and some of them are amongst the oldest methods of internet usage. Bulletin boards, internet forums or newsgroups, and today most blogs, have in common that the template is provided by an ISP, and the content is provided by users. Any user can participate in the discussion, without registration or identification. Postings are spontaneous and sometimes not carefully considered. Some of the earliest significant cases emerged because of bulletin board or Usenet postings (see below *Godfrey v Demon,* and *Stratton Oakmont v Prodigy*). One of the reasons for this is the early popularity of these fora. The other reason is that in this form of communication, there is nobody in charge of moderating or monitoring the content; it therefore seemed natural to make the ISPs responsible.

Today fora are popular tools to attract readers' contributions about any topic of public interest. Beyond some "independent" fora, many are operated by content providers such as news portals, government agencies, or public bodies. Chatrooms are similar to fora but their participants communicate in real time.

2 Weblogs

Blogs, or given their official name, weblogs, are a relatively new trend in internet publication. A blog unifies the features of a website and a forum. Unlike fora, these are not entirely decentralised: there is a person who writes the main thread and who has editing rights. Other people can write comments, but the blogger can moderate comments or allow only certain users to comment. Some blogs attract dozens or more comments, making the site truly interactive. The most popular blogsites carry thousands of blogs.[26] The site and the blogging template is generally maintained by an ISP

---

25 See also *Godfrey v Demon Internet Ltd* [2001] QB 201.

26 In April 2006 there were allegedly 35.5 Million weblogs, the tendency being that their number doubled every 6 months. See http://technorati.com/weblog/2006/04/96.html.

who does not provide content beyond the blog template and instructions on how to set up the blog. Writing a blog instead of building a webpage could be compared to lease: instead of owning a house, it is possible to rent an apartment. The blogsite provides the template for the blog but it does not control content. Blogs can be anonymous or not, and bloggers usually do not reveal more information than their name.

3 Social networking sites, interactive sites

These sites are collections of contributions from thousands of individual users. Rather than forms of individual expression, they allow users to identify themselves as members of a group, in relation to other users. Some sites are built upon providing a special kind of content such as YouTube.[27] Others simply create a virtual social environment.[28]

With the emergence of Web 2.0 user empowerment becomes more and more significant on the internet.[29] Content will be provided by users of the internet community together rather than only by a few identifiable persons.

4 Email

Email is a one-to-one medium, although it can be sent to multiple addresses too. There are no constraints on sending emails to as many addresses as possible, and it is also suitable to spread information to a great number of people. The heading of the email can disguise the actual sender: not only can pseudonyms be chosen, but even the technological meta-data can be falsified to mislead the receiver and the authorities.

The ISP's role here is not more than that of the post to deliver letters. ISPs do not know the content of the emails, and they do not have the right to know. Communication can only be intercepted according to the law and not according to the wish of the ISP.[30]

5 Websites

Publication on a website amounts to publication to the general public. But many websites are accessed only by a few people, often by friends or members of a family. It is not yet decided whether it makes a difference if a website is accessible only by a password, or by subscription. The

---

27 www.youtube.com.

28 www.myspace.com.

29 Web 2.0. is a concept of the future internet application, emerging in 2004 as the name of a series of conferences. It addresses the development of the internet business and software industry, predicting that the next generation of successful internet design patterns and business models will build primarily on user contribution. See www.oreillynet.com.

30 Crimes Act 1961, s 216B.

defendant's website in *Gutnick v Dow Jones*[31] was accessible only by subscription and this did not seem to make a difference for the court. After all, online subscriptions are not different from offline subscriptions or buyers of a newspaper. This could be compared to the membership of a club, in which anybody may become a member. But there are cases where the club does not accept new members, and only a handful of people in fact have the password to access the content. Private websites are only accessible to family or friends. These websites, although literally published, are not as publicly available as a book or a TV show.

The publisher of a website is clearly the person who provides and edits the content, and who usually contracts with the ISP who hosts her content. Some ISPs provide free hosting services, and in these cases the content provider could be anonymous. Both situations raise ISP responsibility in disclosing personal details.

6 Hyperlinking

As John Burrows said: "in New Zealand (...) reference to another person's website can be publication of defamatory material which is to be found on that website."[32] But in one case the Court held that the potential for publication is not publication as such. The fact that records are within easy access is not publication itself.[33] In the case *International Telephone Link Pty Ltd v IDG Communication Ltd*, the court found that references to a website could be sufficient communication of the defamatory contents of that website to constitute publication.[34]

Should the publisher of a link really be liable for whatever appears on the linked page? The information to which the link points can change without notification. A German court has found that the person whose website carries a hyperlink is not liable for the content on the linked page if she did not know and had no reason to know that it carried illegal content.[35]

Often hyperlinking is comparable to recommending a newspaper to someone, without defining which volume and article to read. In other cases, however, the hyperlink can connect to a very specific document. In neither case is there a guarantee that the content behind the link will not change dramatically. Hyperlinking is the spirit of the World Wide Web: without linking we could not use the web. Therefore it is not good policy to discourage content providers from hyperlinking. Just as in the case of hosting services, the subjective factor should be considered, as the German court did.

---

31 *Gutnick v Dow Jones*, above n 23.

32 Todd, above n 17, 826.

33 Todd, above n 17, 827, citing *Henderson v Canterbury Hospital Board* (6 July 1988) CP173/88 HC CHCH.

34 *International Telephone Link Pty Ltd v IDG Communications Ltd* (19 January 1998) HC AK CP344/97, 6 Kennedy-Grant J.

35 *Local Court Berlin-Tiergarten v Angela Marquardt* (1997) 260 DS 857/96.

7 Streaming video and audio

Real-time audio and video content is becoming more widespread and popular on the Internet. Television and radio have been subject to stricter regulation than newspapers traditionally. In its early stages, the internet carried mainly text, then it began carrying more and more pictures. The real explosion of visual and audio content was enabled only by the widespread use of broadband.

The relationship of such content to broadcasting is not settled yet. According to the wording of the New Zealand Broadcasting Act – and a decision of the BSA – real-time streaming content could be "programme".[36] In this case nothing would prevent ISPs from being identified as broadcasters, with all the obligations of a broadcaster.

There is a widely accepted principle in media law that broadcasting should be subject to stricter regulation than printed press.[37] The difference is usually justified by three characteristics of the electronic media. The first is the scarcity of frequencies that were traditionally used for the distribution of television and radio programmes. Not everybody is able to express their opinions through the mass media therefore its editors must maintain a balanced programming structure.[38] The second argument is that electronic media have a stronger impact on public opinion and have a uniquely pervasive presence that intrudes into homes and cars, at every time of the day. It is difficult to control the content which "flows" from the medium, in contrast to the printed press.[39] This latter argument could be regarded as a predecessor to the newer push-pull differentiation between the ways that printed press and electronic media are consumed.[40] According to this, radio and television are distributed by way of a push-type technology and the viewers and listeners perceive it passively. Whereas in the case of the newspaper – along with the internet – content needs to be actively selected by the reader (or user) who must perform a series of actions to confirm her intention to get to the required content.

Technology has neutralised these traditional reasons of stricter regulation. Already cable and satellite television have weakened the scarcity rationale, and, further, with digital television the push distribution may be questioned, whereas there are new uses of push distribution through internet and mobile phone devices. Convergence of technologies complicates the situation further. Regulation of electronic media is bound to experience major changes. This will be discussed further in Chapter II.

---

36 Broadcasting Act 1989 s 2; *Kevin Davies v Television New Zealand Ltd* (31 March 2005) BSA 2004-207.

37 Eric Barendt *Broadcasting Law* (Clarendon Press, Oxford, 1993).

38 *Red Lion Broadcasting Co v FCC* (1969) 395 US 367, 388 White J for the Court.

39 *FCC v Pacifica Foundation* (1978) 438 US 726.

40 Lawrence Lessig "What Things Regulate Speech: CDA 2.0 vs. Filtering" (1998) http://cyber.law.harvard.edu/works/lessig/what_things.pdf.

V LIABILITY OF ISPS IN NEW ZEALAND UNDER THE CURRENT LEGAL RULES IN 2006

Below I will analyse how some relevant laws of New Zealand apply to ISPs. These laws were not designed to deal with the newly emerged intermediaries which ISPs are. Often it requires creative thinking to apply the law to possible situations. Therefore, the outcome of an eventual lawsuit is almost unpredictable. The extent of this study does not allow analysis of all possible legal issues; therefore I select a few typical cases which serve as examples to introduce the problem. To better demonstrate the various problems ISPs face, I divide the issues into categories of civil and criminal liability, where criminal liability is discussed with a special emphasis on absolute liability structures. Copyright will be discussed separately because ISPs are targeted in the pending legislation. Among others, liability for breach of confidence, racial discrimination, and under the Fair Trading Act are also discussed shortly. In the category of civil liability defamation is the centre of focus because it is a good object for examination: it is a lawsuit between private parties, not regulated by contract, and there are small differences between different countries. In absence of New Zealand cases I am confined to illustrating my arguments with foreign examples where the legal environment is or was similar to that of New Zealand.

A Civil Liability with International Examples

1 Single publication rule

Above, various possible templates of Internet publication were discussed. Beyond the usual question of what is meant by "published", a further problem may arise from the traditional common law rule which holds that each publication amounts to a different cause of action.[41] In *Gutnick* Hedigan J held that the publication takes place at the moment the contents "are seen and heard (...) and comprehended by the reader or hearer".[42] As Judge Harvey wrote, "[t]he tort of defamation has always defined publication as occurring when the defamatory meaning is conveyed to a third person, and this can only occur when the message is read."[43] In an internet context this can mean that every time when another user accessed the homepage it counts as a different publication. This was obviously not the case with newspapers which were distributed in thousands of copies, and still the publication was counted as singular. A new publication resulted only if the defamatory information was printed again. If the same – offline – newspaper was read years later accidentally by someone who found it, or in a library by a researcher, it did not count as a new publication. In contrast to this, in *Loutchansky v Times*, the online version of the Times was found liable for a

41 Todd, above n 17, 827-828.

42 *Gutnick v Dow Jones*, above n 23, para 60 Hedigan J. See also David Rolph "Before the High Court: The Message, Not the Medium: Defamation, Publication, and the Internet in *Dow Jones & Co Inc v Gutnick*" (2002) 24 Sydney L Rev 263, 265.

43 David Harvey *Internetlawnz Selected Issues* (LexisNexis, Wellington, 2005) 322.

newly-committed defamation when the defamed person accessed the defamatory site more than a year after the original publication – even though it was not proven that anyone else actually did access it.[44]

News portals operate very similarly to newspapers: they have their front pages and further pages inside. Older content is in archives. Only those who actively look for it can find any of those older articles. Nevertheless, some websites kept by amateur content providers might have less frequent updates, or not have updates at all. This means the information is present on the front page for a long time. On the one hand, online newspapers are in a more burdensome situation because they have to deal with archiving and make sure they make defamatory or otherwise unlawful material inaccessible even in future. On the other hand, it is easier to remove the questionable material from the web than try to withdraw sold copies of a newspaper.

The United States introduced the so-called "*single publication rule*" for defamation in almost all of its states.[45] There have been a few cases discussing whether the single publication rule applies in an online environment, or whether each day the content appears online counts as a new publication. The courts have firmly rejected the latter argument and established that the single publication rule applies online as well, and is counted from the first day of publication.[46]

The United Kingdom does not have such a rule. The New Zealand Defamation Act has a section about "single publication", but its content is different from the American one. Perhaps it reveals the original intention of the single publication rule: "[p]roceedings for defamation based on a single publication constitute one cause of action, no matter how many imputations the published matter contains."[47] This means that the defaming statements published in one edition must be treated as one defamatory statement. It focuses on the act of making statements, rather than on the act of publication. Interestingly, the British courts also held that one publication is one cause of action. This sounds similar to the New Zealand approach. However, the UK court deduced from this that multiple accesses to the same article means multiple publications, that is, multiple causes of action. Despite the seemingly similar words, the latter argument is the opposite of the American rule and does not have any relation to the New Zealand one.

2 Distributors' liability

The main peculiarity in ISPs' role of publication is that they are usually unaware of the content that they carry. This situation is not without previous examples. There is already a legal exemption for librarians and booksellers, who, although they help to distribute the information, do not control it

---

44 *Loutchansky v Times Newspapers Ltd (No 2)* [2001] EMLR 36, 243 (EWCA) Phillips LJ.

45 For example, Rest (2d) Torts § 577A (1977) Single And Multiple Publications.

46 See *Firth v New York* (2002) 98 NY 2d 365 (CA).

47 Defamation Act 1992, s 7.

themselves. No librarian or bookseller is expected to be aware of every piece of information in the books and newspapers. However, once they have been informed about the illegal nature of the publication, they can prevent its distribution. They neither have the right, nor the ability, to edit the published material: they can only ban the edition as a whole. Although an ISP could alter or delete certain selections from a webpage, this would hardly be different from a librarian tearing out pages from a book. The act is destructive not only because it damages the object, but because it interferes with the author's rights. In New Zealand, this exemption appears under section 21 of the Defamation Act 1992:

> 21 Innocent dissemination
>
> In any proceedings for defamation against any person who has published the matter that is the subject of the proceedings solely in the capacity of, or as the employee or agent of, a processor or a distributor, it is a defence if that person alleges and proves--
>
> a) That that person did not know that the matter contained the material that is alleged to be defamatory; and
>
> b) That that person did not know that the matter was of a character likely to contain material of a defamatory nature; and
>
> c) That that person's lack of knowledge was not due to any negligence on that person's part.

These conditions are very similar to those of the British Defamation Act 1996, which is discussed below. However, the wording of the section does not resolve all doubts. As John Burrows puts it: "There is also scope for interpretation in factors (b) and (c). It may be difficult, for example, to decide when a matter is 'of a character likely to contain' defamatory material."[48]

Subsection (B) suggests that the disseminator is expected to make a value judgement about "the matter", which is impossible if he or she – in our case an ISP – does not know about "the matter" at all. In some cases there would be no difference between subsections (a) and (b). Burrows says, that "presumably the previous record of a newspaper, the events occasioning the publication and the reputation of the author might all play a part".[49] One example could be the situation underlying the case *Blumenthal v Drudge*.[50] The case would have resulted in a different outcome in New Zealand. AOL contracted Drudge, who was and still is infamous for his gossip pages and newsletters. Although AOL did not know the content of the publication itself, and left it entirely to Drudge to fill the pages with content, they could have known that his writing was likely to have a defamatory nature.

---

48 Todd, above n 17, 830.

49 Ibid.

50 *Blumenthal v Drudge*, above n 1. A United States case (see in more detail below at 3[e]).

The same argument could make an ISP liable for hosting websites with names that reveal the defamatory nature of their content. In the *Drudge* case AOL even received extra profit from Drudge's defamatory content, because it was intended to attract customers and readers. This is not typical for ISPs who host websites, but the opposite is also possible, as in *UMA v Cooper*.[51]

Also, subsection (c) requires a lack of negligence. Negligence can be judged when the standard of reasonable behaviour is known. In the case of ISPs, however, the problem is that reasonable behaviour is not defined.

Finally, the term "distributor" has a narrow interpretation in the Act. According to section 2 distributor includes booksellers and librians. Altogether, the Defamation Act 1992 does not solve questions surrounding defamation cases regarding ISP liability and leaves room for creative judicial interpretation. As early as 1999 the New Zealand Law Commission came to the same conclusion:[52]

> In our view, there is a need for ISPs to be protected through the innocent dissemination defence provided by section 21 of the Defamation Act 1992. While, in ECom 1, we indicated that an ISP would probably fall within the definition of "processor" and "distributor", on reflection *we tend to the view that the law should be amended to remove any residual doubt.* It is not inconceivable that a judge, interpreting those definitions, could come to the view that they did not include an ISP. Accordingly, we recommend that the problem be solved by including in the definition of "distributor" reference to an ISP. Internet Service Providers should then be defined in a separate definition to include providers of the services discussed in para 242.

The reasonable duty of librarians may also cause surprises. In *Vizetelly v Mudie's Select Library Ltd*,[53] the owners of a library were held liable for having overlooked a publisher's circular recalling the book in question. The situation can be compared to those ISPs who – unintentionally – keep cache copies of illegal content, after a court has declared it illegal, and required them to remove it from the web.

A court in a civil case can issue a decision which obliges everybody who might keep a copy of the content to remove it. Any ISP, who hosts mirror sites or caches of illegal content could be found liable; even if, following the *Vizetelly* case, without knowing that it is content found illegal by the court. This is a further reason why statutory establishment of ISPs' duties might be necessary.

---

51 *UMA v Cooper*, above n 11.

52 New Zealand Law Commission *Electronic Commerce Part Two: A Basic Legal Framework* (NZLC R 58, Wellington, 1999) 269 (emphasis added, citation omitted).

53 *Vizetelly v Mudie's Select Library Ltd* [1900] 2 QB 170, cited by Burrows in Todd, above n 17, 830.

The other statutory defences for defamation are unavailable for ISPs because they can apply only in situations where the person knew what was published.[54] This also underscores that providing internet services should never be treated as publication.

The Defamation Act does not say that the innocent disseminator is not a publisher for the purposes of defamation – it simply says a publisher can avail itself of the defence of innocent dissemination. (Whereas, in the UK Defamation Act 1996, it is a defence if a person is "not the author, editor or publisher".[55]) Also, no court has declared that ISPs were not publishers in New Zealand. Other Acts (the Human Rights Act, the FVPC Act or the Privacy Act) do not enable the use of the defence of innocent dissemination, so ISPs remain without a defence.

The most relevant cases decided under the rule of innocent dissemination are: *Godfrey v Demon Internet*, *Cubby v Compuserve*, and *Stratton Oakmont v Prodigy*.[56] Although the latter two are American cases, they were decided referring to distributors' liability, which is very similar to the innocent dissemination rule.

3 Court cases under the distributors' liability structure

The American courts were the first to use the analogy of the "distributor" or "bookseller", saying that ISPs are just as liable for the content they host as booksellers are, who are not obliged to know the content of all of the books that they offer, but if they are informed that one of them is illegal, they should do everything to remove them and make them unavailable for the public.[57] If they fail to do this, they can be made liable. This was the threshold of liability in the United States until 1996. It is still relevant today, because this liability threshold is very similar to the "innocent dissemination" rule, which is used in the UK and in New Zealand, in the absence of a specific legal exemption.

(a) Compuserve offered content to the public, but the content was written by a contractor's subcontractor, with whom Compuserve did not have a direct contractual relationship. Thus, it had no means of control. Compuserve contracted with Cameron Communications (CC) to run a "Journalism Forum" page. CC delegated this to Don Fitzpatrick Association (DFA) which then wrote and edited the column "Rumorville" within the Journalism Forum. The illegal statement was committed by DFA's director, Don Fitzpatrick. Compuserve and DFA did not have any business relationship with one another; Compuserve paid CC and CC paid DFA. DFA undertook all liability for the statements made in the journal, and Compuserve did not have the chance to control the

---

54 The defences of honest opinion, truth, privilege and consent. See Todd, above n 17, 843.

55 Defamation Act 1996 UK s 1(a).

56 *Cubby v CompuServe*, above n 2; *Stratton Oakmont v Prodigy*, above n 2; *Godfrey v Demon Internet*, above n 25.

57 *Cubby v Compuserve*, above n 2, 139 Leisure J.

content prior to publication. The articles were uploaded by DFA directly to Compuserve's servers. The content was accessible only to Compuserve subscribers, and among them, only to those who specifically subscribed to the column Rumorville at DFA. Compuserve did not get revenues from the subscription fees paid to DFA, it collected only the internet access fee, and the membership fee to the Compuserve network which was paid by all subscribers, including those who did not subscribe to Rumorville. Based upon these circumstances, the Court found that Compuserve was not liable for DFA's writings published through its network.

The Court also referred to *Lerman v Chuckleberry Publishing Inc*[58] which declared that it is a regular practice of New York courts not to hold the seller of a publication liable for its content if the seller does not know, and does not have reason to know, its content"with respect to distributors, the New York courts have long held that vendors and distributors of defamatory publications are not liable if they neither know nor have reason to know of the defamation." [59]

Thus, it confirmed that ISPs' liability is similar to that of booksellers. Although booksellers physically sell the publications, they are not the authors, and it cannot be expected that they read all the books they offer. This exemption would cease when the bookseller is informed of the objectionable nature of a publication, because she is then able to withdraw it, or stop selling it.

This system is very similar to the solution applied by the Directive of E-Commerce of the European Union: ISPs are not liable as long as they do not know and have no reason to believe that the content is illegal. In the *Prodigy* case (see below) the problem was not only that the ISP could have known about the defamatory comment, but that in fact it did more than a normal distributor in that it promised to control content regularly; therefore, the distributors' liability standard could not be applied.

(b) Illegal content can emerge not only in private websites, but also in chatrooms and bulletin boards. These were often monitored and moderated by ISPs, so as to make them more pleasant for their clients. Doing this, these ISPs lost their "innocence" which was necessary to keep them immune from liability. Ironically, those who wanted to act especially expediently lost this immunity and suffered financial damage as a consequence. This happened for example to Prodigy, which ran a bulletin board, where a security investment company named Stratton Oakmont was defamed by a user; Stratton Oakmont was "accused" of having committed securities fraud. Prodigy was sued by the defamed party. Prodigy had advertised its services as being decent, aiming to appeal to millions of American families, and as controlling the content of the bulletin board, doing everything that a responsible newspaper would do to please its readers. Unfortunately, by claiming this, it lost booksellers' immunity. It argued that since the declaration of their policy principles in 1990 the volume of the communication traffic grew to an extent which made it simply impossible to achieve

---

58 *Lerman v Chuckleberry Publishing, Inc* (1981) 521 F Supp 228 (SD NY).

59 Ibid, 236 Werker J.

the original aims. But the court did not accept this argument, saying that it was its own fault in leaving its business policy declaration unchanged.

The court distinguished the case from *Cubby v Compuserve* where the ISP, Compuserve, did not exercise any control at all over the content, and was not in a position to be able to do so. By contrast, Prodigy operated an editorial board to filter out nasty words. This obviously had a chilling effect on communication, but this seemed to be the aim of their policy. The editor acted obviously in the name and to the benefit of Prodigy, unlike in the case of DFA and Compuserve.

This logic meant that Prodigy would have acted without liability if it had not even tried to filter unwanted content, but let the comments be published without any control. This obvious paradox became widely discussed in the professional community, and finally led to the legislation of §230 of CDA, which exempted ISPs from liability for content posted by third parties, whether or not they interfered with the content.

In my opinion, even if Prodigy undertook to filter nasty words from the bulletin board, it could not have judged the truth of such a complex statement. However, it was Prodigy which defined itself as an outstanding company by exercising editorial control, thereby setting unrealistic goals "[c]ertainly no responsible newspaper does less when it chooses the type of advertising it publishes, the letters it prints, the degree of nudity and unsupported gossip its editors tolerate."[60]

Even so, the duties of a moderator are still not settled, and they are not as clear as the duties of a publisher or an editor.

(c) Soon after *Prodigy*'s case, Congress passed the Communication Decency Act,[61] which became notorious because of its unrealistic expectations with respect to pornographic websites. Those sections were annulled by the Supreme Court in a landmark decision.[62] Nonetheless, some of the remaining sections proved to be important in the development of ISP liability.

Declaring an intention to eliminate hindrances from the development of the internet, the "Good Samaritan" provision declares that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider".[63] This immunity is not compromised by applying any measures in good faith, in order to restrict access to or availability of objectionable materials, without regard to their constitutional protection. Neither is it compromised if it provides content providers or users technical means to restrict access to such materials.

---

60 *Stratton Oakmont v Prodigy*, above n 2, para 2, Ain J.

61 47 USCA §223 (a, d).

62 *Reno v ACLU* (1997) 521 US 844.

63 47 USCA §230 (b, c).

These sections were first understood to establish an unconditional exemption for ISPs. Subsection (b) appeared to declare absolutely that under no circumstances can a provider or user be the publisher of content provided by others. However, later cases and authors debated this interpretation, and gradually a new interpretation became accepted. The later construction returns to the distributors' liability and holds that the exemption applies solely where ISPs exercised control over the content in good faith to restrict access to objectionable materials. These opinions will be discussed in more detail in Chapter III.

4 Court cases under the unconditional exemption of ISPs (CDA 230)

(a) CDA §230 was the legal basis in *Zeran v AOL*[64] and *Blumenthal v Drudge*.[65] In *Zeran*, a fake message appeared on AOL's bulletin board advertising T-shirts with "funny" scripts and jokes related to the Oklahoma bombing. This happened about a week after the tragic 1995 Oklahoma bombing where many people, mostly children, died. The forged advertisement gave Kenneth Zeran's name and contact number. He received hundreds of calls from angry citizens to his phone number which had been used in his business, and which he could not use at all for weeks afterwards. His answering machine recorded an outraged message every second minute, among them death threats. He asked AOL to remove the advertisement, which it did, and to publish a retraction – which it did not.[66] The advertisement reappeared four times, each with a slightly different text. When a local radio station gave an account of the appalling advertisement, Zeran phoned in and the station also broadcast his side of the story. Only after a local newspaper published the story in its entirety, did the number of phone calls drop to ten per day. Zeran sued AOL for not publishing the retraction. However, according to §230 of CDA, AOL was not liable for content published by another content provider, who was never found. In my view the real speciality of this case is that Zeran used radio, which is originally a one-to-many medium, in an interactive way, but he did not express himself through the naturally interactive internet. He could have published a retraction himself, instead of demanding one from AOL. In fact, AOL did more than CDA (as it was interpreted at the time) demanded, and could not have been made liable even under the more restrictive notice-and-takedown regime, because it removed the postings as soon as it learned of their defamatory nature. It was absolutely correct not to publish a retraction, since as an ISP it had nothing to do with the postings that the users published. It was probably the new medium's unfamiliar nature which prevented Zeran from replying himself. Zeran was apparently unaware that he could have posted a rectification himself. It might have been even more efficient to publish his reply on the same bulletin board where people read his phone number originally. He tried to communicate with the two media in the same way: to call the representative and ask for retractions. But the internet

---

64 *Zeran No1*, above n 2.

65 *Blumenthal v Drudge*, above n 2.

66 *Zeran No 1*, above n 2, 1127-1128 Ellis J.

bulletin board was not a moderated and edited show like the radio programme. The lack of strict regulation can be justified exactly by this phenomenon: the multitude of information channels. There is no need to convey Zeran's message if he can express himself without a mediator. The right of reply is encoded in the internet communication – everybody may publish their own rectification without requesting it from anyone else: the internet has "a built-in right of reply, so to speak".[67]

(b) The case *Blumenthal v Drudge* is less simple, and very controversial. Drudge was commissioned by AOL to regularly write a gossip column for AOL. Columns were published on his own personal homepage as well AOL's, and he also distributed them through email in his regular newsletter (Drudge Report). He alleged to have had 85,000 subscribers in 1997. In one of his articles he alleged that Sidney Blumenthal, a new White House staff member, had been charged with domestic violence. Blumenthal was to start his White House career the following day, and his wife already worked there. He sent a letter demanding retraction via his lawyer the same day, and Drudge complied with the demand immediately, imparting an extra edition of the newsletter, and let AOL publish the retraction the following day. But Blumenthal then sued AOL and demanded compensation, stating that Drudge acted on behalf of and was commissioned by AOL.

According to the contract between AOL and Drudge, AOL published advertisements of the column to attract more subscribers, and made it accessible to all of its subscribers. Drudge was the writer and editor of the column and updated it regularly.

In contrast to *Compuserve*, there was a contractual relationship between the service provider and the author, and the author acted on behalf of the ISP and was commissioned by it. But §230 of CDA made all such facts irrelevant. Since the content was written not by AOL but Drudge in person, AOL acted only as a service provider; therefore AOL could under no circumstances be regarded as the publisher.

The court made sharp statements while interpreting and analysing §230 of CDA. It emphasised that although §230 was mainly intended for obscene and indecent content, its definition included everything else which might be otherwise objectionable.

It stated that "whether wisely or not, it made the legislative judgment to effectively immunise providers of interactive computer services from civil liability in tort with respect to material disseminated by them but created by others."[68]

It may be observed that the plaintiff first turned to Drudge and not AOL to retract the statement. It is possible that AOL was seen as an attractive deep-pocket defendant, but the plaintiff's first

---

67 Yaman Akdeniz, Clive Walker and David Wall Longman *The Internet, Law and Society* (London, Longman, 2000) However, often the reply may not attract attention equal to the original statement.

68 *Blumenthal v Drudge*, above n 2, 50 Friedman J.

instinct lead to Drudge. It must have been obvious for him who was liable for the infringement and who could retract the defaming statement.

On the other hand, the court did not take into consideration that AOL contracted a notorious gossip author, for the sole purpose of attracting more subscribers. One may ask whether AOL did owe a duty to make a responsible decision when selecting its authors. Particularly, if there was a high likelihood of untrue statements being published, meaning that defamatory statements were foreseeable. Selecting the author was AOL's conscious business decision, in contrast to publishing each piece of writing. The name "Drudge" has become a synonym for untrue information and the problematic area around this.[69] What is more, the Second Restatement clearly says:[70] (emphasis added)

> (A) news dealer is not liable for defamatory statements appearing in the newspapers or magazines that he sells if he neither knows nor has reason to know of the defamatory article. The dealer is under no duty to examine the various publications that he offers for sale to ascertain whether they contain any defamatory items. Unless there are special circumstances that should warn the dealer that a particular publication is defamatory, he is under no duty to ascertain its innocent or defamatory character. *On the other hand, when a dealer offers for sale a particular paper or magazine that notoriously persists in printing scandalous items, the vendor may do so at the risk that any particular issue may contain defamatory language.*

These early American cases represent the main problems that may arise around ISPs' liability in the case of defamation. The United States was the first to develop a legal provision for ISPs' liability. Other countries developed various solutions to the same problem, although the common feature of these is that ISPs should not be liable, at least for what they did not know about. This study will examine some significant solutions and analyse their advantages and disadvantages.

5 *Cases decided under the innocent dissemination rule of the Defamation Act 1996 (UK)*

The landmark defamation case below was decided on the basis of the Defamation Act 1996, before the European Union passed the E-Commerce Directive[71] and consequently before the UK passed the now effective EC Directive Regulations 2002 (UK) (which are discussed in Part III). The Defamation Act 1996 contains some specific sections to protect innocent disseminators, but the ISP in the *Godfrey v Demon Internet*[72] case could not avail itself of the defence. On a scientific Usenet

---

69 Andrew L Shapiro *The Control Revolution: How The Internet is Putting Individuals in Charge and Changing the World We Know* (Public Affairs, New York, 1999) See also www.drudgereport.com.

70 Restatement (Second) of Torts (1976), s 581.

71 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the Internal Market (in short: E-Commerce Directive).

72 *Godfrey v Demon Internet*, above n 25.

newsgroup "soc.culture.thai", an unknown person posted a message which was defamatory of Laurence Godfrey by pretending that it had come from his account, although his name was misspelled as Lawrence. Godfrey faxed Demon and asked for removal of the posting, which did not occur until after the normal fortnightly clearing of messages.

Section 1(1) of the British Defamation Act 1996 defines the defences of innocent dissemination. In section 1(2) it defines the terms "author", "editor" and "publisher" and in section 1(3)(a-e) it lists those who are not to be held publishers. Morland J interpreted section 1(1) so that (a-c) must all be fulfilled. At first sight it may seem that (a) and (b) mutually exclude each other:

> (1) In defamation proceedings a person has a defence if he shows that—
>
> (a) he was not the author, editor or publisher of the statement complained of,
>
> (b) he took reasonable care in relation to its publication, and
>
> (c) he did not know, and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement.

Under section 1(3) an ISP is not to be held a publisher:

> (3) A person shall not be considered the author, editor or publisher of a statement if he is only involved—(...)(e) as the operator of or provider of access to a communications system by means of which the statement is transmitted, or made available, by a person over whom he has no effective control.

It appears that ISPs are not to be regarded as publishers, and by not being publishers they can use the defence specified under section 1(1)(a). As Morland J put it: "In my judgment the defendants were clearly not the publisher of the posting defamatory of the plaintiff within the meaning of section 1(2) and (3) and incontrovertibly can avail themselves of section 1(1)(a)." But he then follows his interpretation of section 1(1) which infers that not only one but all conditions have to be fulfilled. "It should be noted that for the defence to succeed (a) and (b) and (c) have to be established by the defendant. (...) However the difficulty facing the defendants is section 1(1)(b) and (c)."

Morland J found some authority in the consultation document "Reforming Defamation Law and Procedure" issued by the Lord Chancellor's Department in July 1995. This document, among others, held: "The defence of innocent dissemination has never provided an absolute immunity for distributors, however mechanical their contribution. It does not protect those who knew that the material they were handling was defamatory."[73]

---

73 Ibid, 547 Morland J.

Hence, the Judge found that even though Demon was not a publisher, it did not fulfil the requirements of section 1(1)(b) and (c) after it was notified about the defamatory nature, because it chose not to remove the posting. So he concluded that "n [his] judgment the defamatory posting was published by the defendants and, as from 17 January 1997, they knew of the defamatory content of the posting". He thus found Demon liable for defamation, but suggested that any award of damages should be very small.

Notwithstanding the legal importance of the case, it might be an interesting fact that Professor Godfrey is known for his passionate contributions to mailing lists and has initiated several lawsuits against others' allegedly defamatory postings.[74]

B Absolute Liability (Criminal and Civil)

Criminal offences usually require a mental element (*mens rea)*. A perpetrator is generally expected to have committed the act intentionally, recklessly, or with negligence. In these cases ISPs are unlikely to be found liable for contributing to some wrongdoing of which they are unaware. However, they might be found liable for negligence, depending upon their duties. Given that ISPs' duties are not defined, what is understood to be their duties would depend on the courts' interpretation, or, if there is a contractual relationship between the ISP and the content provider, on the declaration of the ISP (like in the *Prodigy* case). Should the ISP declare that it monitors content, or that it will filter out all spam, it could be found negligent if it does not comply with these – unrealistic – undertakings. Without such a declaration, it is up to the court to decide what prudent behaviour is. For the sake of security, the European Directive of E-Commerce declared that ISPs are not obliged to monitor content.

In addition, there are some offences which do not require a *mens rea* at all: these are cases of absolute and strict liability. There is a wide spectrum of opinions criticising this structure, but it is not the purpose of this paper to take a position in this debate in general.[75] However, it may be relevant to note that one of the observations in legal literature is that absolute liability is better

---

74 Godfrey started six libel lawsuits against ISPs during 1997 and 1998, amongst others against Telecom New Zealand: (*Godfrey v Telecom New Zealand and Suradej Panchavinin* [1997] G-No 1071. The others are: *Godfrey v Toronto Star Newspapers Limited and Ken Campbell* [1997] G-No 1036; *Godfrey v Melbourne PC Users Group Inc and Donald Victor Adam Joiner* [1997] G-No 1070; *Godfrey v University of Minnesota, Starnet Communications Inc and Kritchai Quancharut* [1997] G-No 1187; *Godfrey v Cornell University and Michael Dolenga* [1997] G-No 1188; and *Godfrey v Phillip Hallam-Baker* [1998] G- No 2819; see Yaman Akdeniz "Case Analysis: *Laurence Godfrey v Demon Internet Limited*" (1999) Journal of Civil Liberties, 4(2) (July) <http://www.cyber-rights.org/reports/demon.htm> 260-267; See also Carl S Kaplan "English Court May Test US Ideals on Online Speech" (1998) Cyberlaw Journal <http://partners.nytimes.com>; see also Jill Priluck "Free Speech, But Whose?" (1998) Wired www.wired.com/news/politics/0,1283,13467,00.html.

75 See also Clarkson and Keating *Criminal Law: Text and Materials* (4 ed, Sweet & Maxwell, London, 1998) 193-200.

applied in regulatory offences, rather than in stigmatising crimes.[76] Censorship may have been regarded as an administrative issue a long time ago, whereas today being charged with distributing child pornography is highly stigmatising.

Using absolute liability in an offence may serve several purposes. It is supposed to make the prosecution more efficient by making it easier for the judicial procedure to be completed. It may express moral values, aiming to discourage an action which may lead to the offence, to emphasise that whoever engages that kind of action should be aware that she takes the risk of committing an offence. The action is discouraged because it contains the possibility of a more serious offence, for example speeding.[77] The civil objective liability is mostly used so as to make sure that the damaged person can get compensation promptly, even if the person who caused the damage is not to blame morally. Hence it is used most often in connection with operating machines, driving a car, or an aeroplane[78] or otherwise voluntarily engaging in risk-creating activities such as keeping wild beasts.

In case of driving, the restrictions imposed on a driver by making speeding an absolute liability offence are proportionate in the light of the danger posed by a speeding driver. Stigmatising crimes or offences are less likely to attract strict or absolute liability, while morally neutral offences, for example parking offences are more accepted by society to be "simplified" by way of strict/absolute liability.[79]

In the case of publication, one should balance the act of publishing with the perils of objectionable or racial content. Accepting the hypothesis that the legislative rationale of imposing absolute liability is to discourage the action which is risk-creating, one should draw the conclusion that publishing is regarded as a risk-creating activity, and that the legislature would like to discourage people from publishing. However, driving and speech represent different human values and this is relevant from a legal perspective too: "If certain activities are to be protected by means of fundamental rights, then those – particular – activities should not be restricted by offences that permit them only at the risk of uncontrollable criminal liability."[80]

1 Censorship offences

The Films, Videos and Publications Classification Act ("FVPCA") imposes absolute liability on those who supply, distribute, exhibit, display or possess objectionable content. It is no defence "that the defendant had no knowledge or no reasonable cause to believe that the publication to which the

---

76 See also A P Simester (ed) *Appraising Strict Liability* (Oxford University Press, Oxford, 2005).

77 Simester, above n 76, 44.

78 *Civil Aviation Dept v MacKenzie* [1983] NZLR 78 (CA).

79 Simester, above n 76, ix-xi.

80 Ibid, xi.

charge relates was objectionable."[81] Literally, this could mean that ISPs may be found liable if any of their clients used their services to publish objectionable material, because they could not use the defence that they had no knowledge or no reasonable cause to believe that the publication was objectionable. Provided that law enforcement agencies understand the ISPs special situation, this should not happen.

The FVPCA has attracted a wide range of criticism. Among others, the New Zealand Law Society, the Indecent Publications Tribunal and the Department of Justice criticised the absence of a mental element in at least some of the offences.[82] The Act is admittedly in conflict with section 14 of the New Zealand Bill of Rights Act 1990 (BORA), but this does not mean a fatal constitutional conflict in New Zealand. The interpretation of the Act in relation to the BORA was discussed at various instances in *Moonen v Film and Literature Board of Review*.[83] The Court of Appeal dismissed the Board's argument and the High Court's ruling. These were that even if the law is inconsistent with the Bill of Rights, there is nothing for the courts to do, because section 4 prevents the courts from challenging laws on the basis of inconsistency with the BORA.[84] The Court of Appeal called attention to section 6 and its appropriate use, that where more than one interpretation is possible, the courts are obliged to choose the one which is less restrictive on freedom of speech.[85] The Court particularly did not accept that: "Any section 6 softening would be contrary to Parliament's intentions".[86] Rather, the Court of Appeal held:[87]

> the existence and extent of such censorship may indeed be matters to which section 6 is relevant. The censorship provision must be interpreted so as to adopt such tenable construction as constitutes the least possible limitation on freedom of expression.

It also gives directions, as to how section 6 should be applied in the present case. The words "promotes or supports" have a certain flexibility of interpretation, and the Board and the Courts shall use the interpretation which "impinges as little as possible on freedom of expression".[88]

---

81 Films, Videos, and Publications Classification Act 1993 [FVPCA], ss 123(3), 127(3), 129(2), 130(3), 131(3). S 125(3) has a slightly different wording but the same effect.

82 Dean Knight "An Objectionable Offence: A Critique of the Possession Offence in Films, Videos and Publications Classification Act 1993" (1997) 27 VUWLR 451.

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

84 Ibid, 11 Tipping J.

85 Ibid, 16 Tipping J.

86 Ibid, 21-22 Tipping J, citing the Board in the *News Media* case, *News Media Limited v Film and Literature Board of Review* (June 11 1997) HC, Full Court WN AP 197/96, 420.

87 *Moonen*, above n 83, 23 Tipping J.

88 Ibid, 27 Tipping J.

In fact, the risk is so incalculable for ISPs that if they acted responsibly, they should close their businesses. As Sir Peter Berger, Bursar of Selwyn College in Cambridge, said when he resigned:[89]

> [A]s the law stands concerning food hygiene and health and safety [he] were almost certain to be convicted if anything went wrong in the College or its kitchens, and this was so irrespective whether anyone was actually at fault.

As discussed above, the usual policy reason of imposing absolute liability is to discourage an action which is held as risky or immoral by society. Discouraging speech is widely known as a "chilling effect" and is usually not regarded as positive, but as a negative phenomenon. If publishing becomes unreasonably risky, this significantly overrides the acceptable threshold of chilling effect.

Prima facie it is not entirely clear whether the no-defence clause applies to simply ignorance of the law, or ignorance of fact also. According to the Office of Film and Literature Classification, ignorance of the fact of possession is accepted as a defence, if it can be proven beyond doubt.[90] This would mean that it is only an ignorance of the legal qualification of the objectionable content which is irrelevant for censorship purposes. But there would be no need to address this specifically because ignorance of law is not a defence as the ancient principle: *ignorantia legis non excusat*[91] has long expressed. In any circumstances, such a person could hardly argue that she had "no reasonable cause to believe that the publication (...) was objectionable".

The Court stated in *R v Cox* that possession involves two elements: actual control of the publication and awareness that the substance is in his possession.[92] In *Goodin v Department of Internal Affairs* the High Court found that the defendant does not need to know a publication is objectionable, she only needs to be aware of its presence.[93] This approach might have been reasonable under traditional methods of publication. But ISPs actually do not have the slightest information about the content that they host, carry or cache copy. Even bookkeepers or librarians, who are often used as an analogue to ISPs, would have a good chance to at least catch a glance of the publication which is kept by them, before putting them on the shelves, even if they would not, and are not expected to, read them.

This problem was addressed by legislation in February 2005 when an amendment was passed. This exempted ISPs from distributing objectionable material by merely providing access to it. Technically, it redefined distribution so that throughout the sections 123-132 the word "distribution"

---

89 Simester, above n 76, vii.

90 Interview with David Wilson, Information Unit Manager of the Office of Film & Literature Classification (20 July 2006).

91 Ignorance of the law is not an excuse.

92 *R v Cox* [1990] 2 NZLR 275, 278 (CA) Hardie Boys J.

93 *Goodin v Department of Internal Affairs* [2002] BCL 816.

shall not include facilitating access to the publication; and that a person is not deemed to distribute a publication unless the person knows what, in general terms, the publication is or contains:[94]

> However, a person does not **distribute** a publication unless the person
>
> intends, or knows of, the act of distribution; and
>
> knows what, in general terms, the publication is or contains.

Adding:[95]

> (3) 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—
>
> delivery of the publication in physical form; or
>
> transmission (other than by broadcasting) of the contents of the publication.
>
> (4) Examples of a person facilitating access to a publication in the ways referred to in subsection (3) are—
>
> a postal operator or courier providing only some or all of the means necessary for delivering the publication in physical form; and
>
> a network operator or service provider providing only a network or facility through which the contents of the publication are transmitted.]

It may sound surprising that only providing access was addressed here. Apparently, this was the activity which caused the most concern to ISPs that made submissions. This is even though submissions also referred to hosting activity.[96]

Other interpretations of the Act reveal further safe harbours for ISPs. For example, the word "supply" shall be interpreted as meaning "to sell, or deliver by way of hire, or offer for sale or hire". None of these activities are usually performed by ISPs, therefore "supply" is not relevant to them. However, the Act penalises several further activities, such as possession, display, or otherwise deal with (...a restricted publication otherwise than in accordance with its classification) or exhibit an objectionable publication. All of these are absolute liability offences.[97] The question is whether a law enforcement agency would find an ISP's action of *hosting* as "displaying", "exhibiting" or "possessing". These words are not specifically defined by the Act's interpretation provisions (some

---

94 FVPCA, s 122(2) (emphasis in original).

95 Ibid, s 122(3,4) (emphasis in original).

96 Submission on the Films, Videos, and Publications Classification Amendment Bill To the Government Administration Committee, by Telecom Corporation of New Zealand Limited, 10 May 2004.

97 FVPCA, above n 96, ss 123 (1)(b)(f), 125, 127, 131.

of them are defined when in special context). The word "exhibit" is interpreted in special contexts: first in relation to sound recordings where it means the playing of a sound recording; second, as in "exhibit to the public", where it relates to films. None of these special contexts are relevant to ISPs, however, the general (that is, not special) meaning of the word can still apply to their activity.[98] (In other contexts, such as exhibiting pictures I understood that the common use of the word "exhibit" prevails.) The interpretation of the word "display" is given only where it stands as "public display".[99] Section 123(4) includes electronic means under the meanings of "supply", "distribute" or "import". Might this mean that other words such as "display" or "exhibit" do not include in electronic form? Although logically this would follow from the fact that they are not included in the extension, it is very unlikely. The general meaning of these words is likely to include ISPs' usual activity of providing hosting services, and creating cache copies for easier transmission. ISPs perform these activities intentionally, and some of these for profit. Although they do not know what content they host, they know that they carry some content. This may be enough to be found liable under the "no defence" terms of the Act.

There is no way an ISP can make sure that no objectionable content is mixed among the content it hosts or caches. Even if they acted with extra care and did not provide hosting services to any "suspicious-sounding" domain name, and even if they regularly checked the hosted material, they could be found liable for objectionable material that escaped their attention.

Below I outline a list of the possible offences that may threaten an ISP – unless it is assumed that neither display nor exhibition can be realised by means of electronic communication, which is unrealistic in our present day information society:

(a) Based upon section 123(1)(b)(f), an ISP may commit an offence by -

  i) making a copy of an objectionable publication for the purposes of display, or exhibition to any other person. This could happen, for example, by caching.

  ii) hosting an objectionable publication, thereby effecting "display or exhibition (...) in expectation of payment or otherwise for gain".

(b) Based upon section 125(1)(a), an ISP may commit an offence by exhibiting or displaying or otherwise dealing with a restricted publication "otherwise than in accordance with the classification assigned to that publication under [the] Act". Since an ISP does not know that the publication is objectionable, it cannot provide for its display or exhibition in accordance with the classification. Again, although the offence is committed by the content provider, the ISP's liability is not excluded.

---

98 Ibid, Part 1 s 2.

99 Ibid.

(c) Based upon section 127(1) an ISP may commit an offence by exhibiting or displaying an objectionable publication to any person under the age of 18 years. An ISP can always count on having young persons among its users, therefore simply by hosting objectionable content it takes the risk that minors have access to that content as well.[100]

(d) Based upon section 131(1) an ISP may commit an offence by hosting objectionable material, if hosting is found to effect "possession" of the material. The section allows a defence if it happens with lawful authority or excuse, but ISPs do not currently have such an excuse. Although subsections (4) and (5) of the same section provide for exceptions, neither of them mentions or refers to a service provider.

To sum up, it can be observed that although the legislation exempted ISPs from liability as far as they provide *access* to content; it did not exempt them from hosting or caching objectionable content. It is a widespread view that the law enforcement agencies in New Zealand would understand the role of ISPs and not prosecute them unnecessarily. The only question which remains is how a rule which is not enforced affects the legal system and respect for the law.

One additional side-effect of this absolute liability is that it provides an incentive for ISPs to remove objectionable material promptly, once they encounter it. This may sound practical from a law enforcement point of view, but it keeps ISPs under unnecessary pressure. Also, one could argue that some paedophiles might act as their own ISPs[101] and disguise their identities as content providers to escape from law enforcement. The interests of law enforcement can be realised by creating an administrative obligation for ISPs to remove illegal content once they become aware of it, under the threat of a moderate monetary penalty. This alternative would achieve the same goal without the unnecessary stifling of their freedom.

Regulation as it is now makes it unreasonably risky to distribute material of unknown content. It is probably meant to be efficient, but the final outcome is the opposite, because this legislation does not help single out those perpetrators who may be harmful to society.[102]

2 Breach of Privacy

In New Zealand there has been a growing focus on the legal protection of privacy in the past decade. Partly, there has been a gradual recognition of the separate tort of invasion of privacy.[103]

---

100 See also *Reno v ACLU*, above n 62.

101 For example by running their servers or by establishing a blog and post objectionable material in form of comments, or host a forum in their website and post objectionable material, while disclaiming liability for the posting.

102 HL Packer "Mens Rea and the Supreme Court" (1962) Sup Ct Rev 107, 109, cited by Dean Knight "An Objectionable Offence: A Critique of the Possession Offence in Films, Videos and Publications Classification Act 1993" (1997) 27 VUWLR 451.

103 Todd, above n 17, 921.

The *Tucker* Court recognised a tort of public disclosure of private facts.[104] The Privacy Act 1993 established a wide protection of privacy. In *P v D*, Nicholson J set out a four-step criterion that should determine whether a publication is an unlawful invasion of privacy.[105] Further, some other statutes have occasional protective provisions that protect the privacy of a person.[106]

In the case of ISP liability only those privacy infringements which are typically committed by way of publication are relevant, or otherwise those revealing private facts – rather than peeping into a dwellinghouse, for example.[107] These can be among others: disclosure of proceedings of certain courts without permission, disclosure of suppressed evidence, or violation of name suppression orders.[108] This paper does not discuss offences which can be committed only intentionally or recklessly, such as the infringement of the Clean Slate Act 2004 or harassment committed through email.[109] In the first case, information published on a website about someone's criminal conviction becomes automatically illegal after the lapse of seven years. In the second case, if someone is harassed through unsolicited email messages and wishes her ISP to terminate them – it should be made clear that ISPs cannot undertake liability for the content of messages, even if they promised so for marketing purposes.[110] Further, ISPs could get involved in cooperating in unlawful interception, or the unlawful disclosure of (lawful) interception.[111] But again, these can be committed only knowingly, and therefore they fall outside the focus of this research.

The Privacy Act lists twelve privacy principles.[112] The relevant ones are Principles 10 and 11 (limits on use and on disclosure of personal information). An ISP can become an innocent intermediary in violating these principles.

The Privacy Act is not enforceable in a court of law. Instead, complaints may be filed with the Privacy Commissioner, who may attempt to achieve a settlement between the parties.[113] If this

---

104 *Tucker v News Media Ownership Ltd* [1986] 2 NZLR 716, 734 (HC) McGechan J.

105 *P v D* [2000] 2 NZLR 591 (HC).

106 Todd, above n 17, 925. See also Crimes Act 1961 ss 216A-216E, Summary Offences Act 1981 ss 29-30, Postal Services Act 1987 s 14.

107 Although opening an email or a making secret recording could be a relevant prohibition for ISPs. See Crimes Act 1961 ss 216A-216E.

108 Family Proceedings Act 1980, s 169; Children, Young Persons, and Their Families Act 1989, s 438; Evidence Act 1908, s 23AA; Criminal Justice Act 1985, s 140; see also Todd, above n 17, 926-927.

109 Summary Offences Act 1981, s 21.

110 ISPs who promise this could get into a similar situation as Prodigy, Inc in *Stratton Oakmont v Prodigy*, above n 2.

111 Crimes Act 1961, s 216B, s 312K.

112 Privacy Act 1993 s 6.

113 Ibid, s 74.

attempt fails, the Commissioner may refer the complaint to the Director of Human Rights Proceedings to decide whether the matter should come before the Human Rights Review Tribunal.[114] Aggrieved individuals may also bring their complaints to the Tribunal.[115] Once a privacy complaint comes before the Human Rights Review Tribunal, it is not a defence that the interference with privacy took place unintentionally or without negligence:[116]

> It shall not be a defence to proceedings under section 82 or section 83 of this Act that the interference was unintentional or without negligence on the part of the defendant, but the Tribunal shall take the conduct of the defendant into account in deciding what, if any, remedy to grant.

Similarly to the FVPCA, nothing protects ISPs from being summoned before the Privacy Commissioner or the Tribunal if other conditions are met; even if the plaintiff and everybody else is aware that the interference was not intentional, and the ISP did not even breach any duty in letting it happen. A plaintiff may have a reason to do so, if the actual content provider is anonymous and is never found; or, if although known, no damages can be expected from her. A deep-pocketed ISP can be an attractive defendant in such case.

The Commissioner and the Tribunal both have the discretionary right to take into account the circumstances of the defendant,[117] and in such case probably they both would decide that the ISP was an innocent contributor who cannot be held liable. However, even this far the ISP could incur costs and inconvenience related to the proceedings, not to mention anxiety caused by the anticipation of damages that may be awarded.

However, the question may emerge, whether the Privacy Act applies to internet-related activities at all? According to section 2, an agency is "any person or body of persons, whether corporate or unincorporate, and whether in the public sector or the private sector". Therefore an ISP can be regarded as an agency. The same section excludes all news media from having to comply with the Act in relation to its news activities, and defines news activity and news medium. It may be doubtful whether news portals would count as "news medium". It is not yet settled whether internet news portals would be regarded as newspapers, as television, or radio, respectively. However, in issues related to privacy the Act gives a definition of news medium as meaning "any agency whose business, or part of whose business, consists of a news activity; but, in relation to principles 6 and 7, does not include [...] Television New Zealand Limited."[118]

---

114 Ibid, s 77(2).

115 Ibid, ss 82(2), 83.

116 Ibid, s 85.

117 Ibid, ss 71, 85(4).

118 Ibid, Part 1 s 2(1).

This definition is technology-neutral; therefore it can be held relatively safely that it would include news sites.[119] A further definition clarifies what news activity is:[120]

> a) The gathering of news, or the preparation or compiling of articles or programmes of or concerning news, observations on news, or current affairs, for the purposes of dissemination to the public or any section of the public:
>
> b) The dissemination, to the public or any section of the public, of any article or programme of or concerning—
>
> (i) News:
>
> (ii) Observations on news:
>
> (iii) Current affairs:

This definition is wide, and it may also include those non-corporate sites which provide observations on news, such as blogs, or which carry specified current information in a certain field of interest (for example <www.news.com.com>). However, the internet hosts hundreds of activities other than gathering or publishing news, which are therefore not exempted. Some of the sites carried by ISPs may fall into the blurred area, being unclear whether they qualify as a news medium or not, for example blogs. ISPs are not expected to know the content of the sites and make a judgement as to their category. As a result, they cannot know whether a site falls under the Privacy Act or not.

The Broadcasting Act imposes an obligation on broadcasters to respect the privacy of the individual, independent of whether they broadcast news or other programmes.[121] As indicated above (and discussed in details later under C), under the current wording of the Broadcasting Act streaming (real-time) internet audio and video content could be taken as broadcasting. Nothing excludes that an ISP is a broadcaster of such content – although this is unlikely.[122]

A further theoretical question may be whether an ISP is the actual "holder of the information"? The privacy principles set requirements for agencies "that hold personal information" or that collect personal information. Even if an ISP does not collect information actively, when a website contains personal information it is not excluded that the ISP, by having control over the transmissions of the website, can be regarded as holding that information.

---

119 Although the definition uses the word "agency" as a basis, the same act gives a definition of agency which excludes news media from being agencies: "agency- (b) Does not include- (...) (xiii) in relation to its news activities, any news medium." However, the intention of the legislature is clear, therefore this contradiction will be ignored here.

120 Privacy Act 1993, Part 1 s 2(1).

121 Broadcasting Act 1989, s 4(1)(c).

122 Ibid, s 2(1).

The principle which could be the most relevant for ISPs is Principle 11: "[l]imits on disclosure of personal information". If a content provider published information in breach of the Privacy Act, its ISP might be regarded as providing the facilities for that. Other principles may become relevant too. In fact, if a user or content provider breaches any privacy principle, the ISP could be regarded as contributing to it.

Provided that an ISP monitored the content it hosted, and found content which could potentially violate the privacy principles, it would not know enough about other circumstances to decide whether the information is in fact provided unlawfully or lawfully. Even if it could easily decide that the site does not qualify as news media, it still would not know the reasons and justifications behind the act of collecting or imparting information; whether the personal information is disclosed for the lawful purpose that it has been collected, or with the consent of the individual, or for another lawful reason.

Consequently, it seems necessary to treat ISPs as independent third persons who have neither control nor awareness about violation of privacy rights committed by the content provider.

3 Breach of confidence

Breach of confidence has some relationship to privacy and issues of confidentiality, notwithstanding there are no strict liability issues. Breach of confidence has been established mostly where there was a relationship between the parties, namely where one party owed a duty of confidence to the other. it is unlikely that an ISP will be sued for breach of confidence, unless of course it had entered into such a contract, for example with its users.

Sometimes the confidential nature of the information ought to be obvious to everybody. Even then, an ISP would be not aware of the circumstances of the case. Even if an ISP knew about the content in question – for example because it would have been notified – it is not in the situation to know whether (a) the information is published with the consent of the person entitled to dispose of the secret, or (b) the information has been publicised earlier, thus losing its confidential nature – as in the famous *Spycatcher* case.[123]

4 Offences against the Human Rights Act and race relations

Similarly to the FVPCA the Human Rights Act (HRA) establishes absolute liability offences. It is no defence that a breach of the Act was unintentional or without negligence, although the Tribunal must take it – among other factors – into account, when it decides what, if any, remedy to grant:[124]

---

123 *Observer & Guardian v The United Kingdom* (1991) 14 EHRR 153.

124 Human Rights Act 1993 (HRA), s 92(4).

> (4) It is no defence to proceedings referred to in subsection (2) or subsection (5) that the breach was unintentional or without negligence on the part of the party against whom the complaint was made, but, subject to section 92P, the Tribunal must take the conduct of the parties into account in deciding what, if any, remedy to grant.

In the international environment that the internet represents the most relevant provisions may be sections 61 and 63: racial harmony and racial harassment. These can be committed without targeting any specific person. It is unlawful to publish:[125]

> [W]ritten matter which is threatening, abusive, or insulting, or to broadcast by means of radio or television words which are threatening, abusive, or insulting (...) and (...) likely to excite hostility against or bring into contempt any group of persons in or who may be coming to New Zealand on the ground of the colour, race, or ethnic or national origins of that group of persons.

Although less typically, breach of other sections of the HRA can become relevant as well, for example section 62 relating to sexual harassment. That section prohibits the use of language of a sexual nature, to subject "any other person to behaviour that is unwelcome or offensive (...) and is repeated or has a detrimental effect on that person." Sexual harassment typically would be targeted against one certain person, but discriminatory speech alone without targeting any specific person can similarly be offensive.

The internet is used not only to express ideas but also for more practical matters, such as the job applications, applications to education institutions, and shopping. Discriminatory behaviour is possible in provision of goods and services,[126] or by advertisement.[127] The absolute liability clause of the Human Rights Act, which may bring ISPs into the unpleasant situation of being liable for offences that they are not to blame for.

It could be argued that the nature of these offences means that an ISP can decide at first sight whether the offences are unlawful or not. Unlike defamation or privacy violations, this unlawfulness is objective, because it does not depend on the victim's perspective. Indeed they might establish with relative certainty that a matter is offensive or discriminatory. However, given the long list of exceptions, for example in employment matters, or the possible artistic or literary merit of the expression, the situation may be more complex. A final decision on the lawfulness of such speech can only be delivered by the courts, and until then it remains uncertain. The provisions of the Act are sufficiently narrowly tailored so that using some racial epithets alone would not amount to a breach of sections 61 or 63. This is because repetition or harmful effect of the offensive language is also required. It is also possible that the questionable content carries literary or artistic value, or is a

---

125 Ibid, s 61(1).

126 Ibid, s 44.

127 Ibid, s 67.

provocative formulation of the person's political opinion, and although prima facie offensive, does not breach the law, or is not against the public interest.[128] The FVPCA acknowledges this as an exception by ordering that when deciding whether material is objectionable, it should be considered whether the material has a literary, artistic or other merit; and likewise in some other sections.[129] The HRA does not acknowledge the same, however, the last condition for the offences in the HRA ("either repeated, or of such a significant nature, that it has a detrimental effect on that person") possibly excludes those materials that have some social merit. In such cases, removal of the material would be a serious restriction of freedom of expression, and by balancing the two rights – the right not to be discriminated against and the right to freedom of expression – the latter may prove to be more substantial. Therefore automatic removal of suspicious content should not be regarded as a solution. But it should depend on the circumstances: whether the author is named, whether the material represents any real value and is more than just a spontaneous comment on a bulletin board.

5 Fair Trading Act

The Fair Trading Act 1986 also lists a number of offences that can be committed through publication. One of the defences is that:[130]

> (i) The contravention was due to the act or default of another person, or to an accident or to some other cause beyond the defendant's control; and
>
> (ii) The defendant took reasonable precautions and exercised due diligence to avoid the contravention.

The two conditions apply jointly, and although the first one very clearly applies to ISPs, the second one leaves doubt. What precautions would be reasonable and what is the diligent behaviour expected from ISPs? This, among others, should be clarified by legislation when making a general statement about ISP liability.

The Fair Trading Act provides a specific defence if it is the defendant's business to publish advertisements and the defendant had no reason to suspect that the publication of the advertisement constituted a contravention to the Act.[131] This reveals an intention that intermediaries should not be held liable.

---

128 For example, as in the film "Cabaret" (directed by Bob Fosse).

129 FVPCA, above n 96, ss 3(4)c, 23(3), 44(3).

130 Fair Trading Act 1986, s 44(1)(c).

131 Ibid, s 44(4).

C Copyright

Relevant copyright legislation has been discussed and drafted in New Zealand in the past years. Shortly before finishing this paper, the Copyright (New Technologies and Performers' Rights) Amendment Bill (the Bill) has been issued.[132] Below I give an explanation of the current situation to show why the amendment is necessary, and later analyse the Bill as it appeared on 7 December 2006. Beyond other elements of a comprehensive amendment, the Bill also completes the Act with a few additional paragraphs which specifically address ISP liability. The slight amendments in the definitions do not affect ISPs (for example, section 2 or sections 35-37).

In other countries legislation had clarified the exemption that ISPs enjoy today, courts have found ISPs liable for copyright infringements on several occasions, but in New Zealand this has not occurred.[133] ISPs are favoured targets of litigation even today, because of their better financial situation and easy availability compared to an anonymous user.[134] Despite the general acceptance of exemptions, copyright holders are inventive in how to impose pressure on ISP defendants by legal threats.[135]

The notice-and-takedown systems (described later) are based upon the principle that the ISP is not liable unless it knew or had reason to believe that it infringed copyright. However, for ISPs it makes a significant difference whether there are specific provisions exempting them from liability or not. First, legislation may clarify that ISPs are absolutely not liable for providing access to copyrighted material or for transient copying, because the condition applies only for hosting and searching services.[136] Second, if there is a legal exemption then the burden of proof is transferred from the ISP to the plaintiff. A legislative instrument may also define the duties of ISPs, or the lack of duties: for example, the European E-Commerce Directive declares that ISPs are not obliged to monitor content.[137]

The law of copyright is dramatically affected by the emergence of new technology. Copying and distributing copies became ubiquitous, and it is difficult to imagine life without at least some forms of copying. Intellectual property has been also a trigger for legislation about internet issues in

---

132 See New Zealand Parliament – Bills.

133 See *Religious Technology Center v Netcom, Inc* (1995) 907 F Supp 1361 (NZ Cal). See also *Hallyday v Lacambre*, 1999 Cour d'Appel de Paris, or *MAI systems v Peak Computer* (1993) 991 F 2d 511 (9th Cir), referred to in Susy Frankel and Geoff McLay *Intellectual Property in New Zealand* (LexisNexis Butterworths, Wellington, 2002) 734.

134 Frankel and McLay, above n 133, 709.

135 See the latest Google lawsuit; Declan McCullagh "Nude-photo site wins injunction against Google" (21 Feb 2006) www.news.com.com.

136 And, under certain circumstances, caching services. See 17 USCA §512.

137 Directive, above n 71, Article 15.

general and among them ISP liability. There has been considerable pressure on governments from powerful stakeholders to deal with this question, even ahead of other, similarly important questions, such as internet defamation or child pornography. Copyright may well be the only area in internet communication which is already governed by international treaties.

1 Primary and secondary infringements

Under the Copyright Act 1994, ISPs could be held liable for both primary and secondary infringements of copyright. In the case of primary infringements, not knowing that the material was protected by copyright is not a defence. Currently, even transient copies are infringing, because of the definition of copying:[138]

> copying-
>
> (a) Means, in relation to any description of work, reproducing or recording the work in any material form; and
>
> (b) Includes, in relation to a literary, dramatic, musical, or artistic work, storing the work in any medium by any means;

The Bill proposes to amend subsection (d) of the definition which does not affect ISPs. In the case of secondary infringements, the Act requires a knowledge element: that the person knew or had reason to believe that the copyright infringement is taking place.[139] This provision remains similar in substance in the Bill also.

2 The New Zealand Copyright (New Technologies and Performers' Rights) Amendment Bill

During the consultation period, a MED Discussion Paper explained why there is a need for regulation and the main principles for regulation. It said that in the absence of specific regulations ISPs face legal liability for copyright infringement.[140] Potential liability could arise where ISPs engage in caching;[141] in situations where they could be said to have authorised further copies being

---

138 Frankel and McLay, above n 133, 734; see also Copyright Act 1994, s 2.

139 Frankel and McLay, above n 133, 235; Copyright Act 1994 ss 35-37.

140 Ministry of Economic Development Discussion Paper (MED Discussion Paper) "Digital Technology and the Copyright Act 1994: a Discussion Paper" (10 Jul 2001) D. Liabilitiy of Internet Service Providers for Copyright Infringement.

141 Ibid, 141.

made by users;[142] for simple transient copying in the course of providing access services;[143] and for maintaining bulletin board services, where the ISP monitored the service.[144]

In government and industry there seemed to be a general understanding that a limitation of ISP liability for both primary and secondary copyright infringement was necessary.[145]

3 Reflections on the Bill

The drafter has chosen a minimalist approach to regulation. The Bill follows the usual structure of ISP liability legislations: it addresses access, hosting and cache. It does not address searching services, similarly to the European Directive (see below), although this exemption may be necessary too, as it was shown in a recent case where a search engine provider was sued for providing links in their search result page.[146] But an analysis of the DMCA practice showed that a notice-and-takedown service for searching services is often misused: malicious notices are sent to search engine providers aiming at removing links to competitors.[147]

The Bill exempts ISPs from liability if a user infringes copyright by using their services.[148] It declares unaffected a copyright owner's right to ask for an injunctive relief, similarly to the E-Commerce Directive or the DMCA. Then it exempts ISPs from liability for storing infringing material, with the following conditions: the ISP does not modify the material; it does not know and has no reason to believe that the material infringes copyright; and as soon as possible after it becomes aware of the infringing material, deletes it or prevents access to it.[149] This latter provision is also similar to the laws mentioned above. The user shall be notified of the deletion as soon as possible. Following this, the Bill discusses exemption from liability for caching material.[150] The MED Discussion Paper had recommended exemptions from liability in the case of caching, including not only automatic caching, but also selective caching to help access to certain pages.[151]

---

142 Ibid, 142.

143 Ibid, 143.

144 Ibid, 144.

145 MED Cabinet Paper "Policy recommendations of the Digital Technology and the Copyright Act 1994" (25 June 2003).

146 Google lawsuit, above n 135.

147 Jennifer M Urban and Laura Quilter "Efficient Process or Chilling Effect? Takedown Notices under section 512 of the Digital Millenium Copyright Act" (2006) 22 Santa Clara Computer & High Tech L J 621.

148 Copyright (New Technologies and Performers' Rights) Amendment Bill [Bill], s 53, "92B".

149 Ibid, s 53, "92C".

150 Ibid, s 53, "92D".

151 MED Position Paper "Digital Technology and the Copyright Act 1994" (Dec 2002) 85.

However, the Bill's proposal on caching does not reflect this extensive interpretation. Cache is defined as a storage that is automatic, temporary, and "for the sole purpose of enabling the internet service provider to transmit the material more efficiently to other users of the service on their request."[152] This does not say, at least not explicitly, that ISPs are allowed to select those pages consciously that are frequently accessed and cache them.

On the other hand, it creates a wider safe harbour for ISPs as it does not require that they comply with the updating policy of the website, or with the conditions on access to the information. However, these measurements – especially the latter one on conditional access – may be found necessary by the internet content industry.

The Bill's exemptions apply to ISPs only if they have adopted and reasonably implemented a policy that provides for termination of the accounts of repeat infringers.[153] It is not defined what counts as repeat infringement or who defines this. Theoretically only infringements that have been established by court ought to be counted. An analysis of the DMCA practice showed that copyright owners tend to notify ISPs about repeat infringements who then feel obliged to terminate the user's account immediately, without investigating the truth of the claims. Termination of an account is a rigorous sanction considering the following facts: only two alleged infringements may result in termination; the user is not notified in advance; an internet account may be used for work or to access public services, by more members of a family. Considering an imaginary but not unlikely scenario where a ten-year-old uses file-sharing software and consequently the family's internet access is terminated without notice, this sanction may be regarded as disproportionate. A further circumstance may be that many users conclude a fixed term contract with their broadband internet service provider in which case early termination of contract attracts a penalty payment. It is questionable whether all these consequences were kept in mind when the above provision was drafted.

The Bill has not addressed the problem of peer-to-peer applications. If infringement occurs every time a protected music file is downloaded, then using a file-sharing application results in repeated infringements immediately. Even where an ISP is aware of the infringing behaviour of the user, it does not have a choice of notifying her before terminating the account. Further, the effectiveness of this penalty is not proven. The issue is discussed in more detail in Part IV.

D Internet Content's Relation to Broadcasting

1 ISPs' role in webcasting

The word "broadcaster" has a fairly stable and unambiguous meaning in common language. However, since more and more audio and video programmes are transmitted through the internet,

---

152 Bill, above n 152.

153 Ibid, s 53, "92D(4)(c)".

either real-time, or downloadable, it is worthwhile examining the overlapping notions of ISPs and broadcasters.

When the Broadcasting Act was designed, the legislator could not foresee the rapid growth of the Internet. Therefore the definitions and terms of the Act neither include nor exclude the internet as a way of transmission. Simply interpreting the provisions will not give a definite answer as to whether or not audio and video content transmitted through the internet could fall under the Broadcasting Act or not. However, the Broadcasting Standards Authority issued a decision in 2004 in which it interpreted the Act to this effect and came to a reassuring result. It found:[154]

> Downloadable content from a website differs from much other internet content in one important respect – it is viewable only once the user has specifically chosen to download and view it, usually through clicking on an icon on the relevant webpage. The material is not continually being shown on the website, regardless of whether users choose to view it, in the same manner that television stations broadcast irrespective of whether the audience chooses to watch.

Therefore, the Authority interpreted the act of clicking on the icon as a "request" to get the information downloaded onto the viewer's computer; once downloaded, it formed the viewer's possession, to be viewed only by him or her. The BSA used subsection (a) of section 2 of the Broadcasting Act to reach this conclusion:[155]

> Broadcasting means 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.

Hopefully, the BSA decision firmly laid down the principle to treat internet content outside the scope of the Broadcasting Act. One could argue that downloadable content is accessible to anyone who wants to download it, and is not more individual than television content that is accessed as the viewer navigates to the desired channel. For example, a Scottish court in the case of *Shetland Times Ltd v Wills and another* held online journals to be "cable programmes" under the Copyright, Designs and Patents Act 1988 (UK).[156] The Act in question provided that:[157]

---

154 *Kevin Davies v Television New Zealand Ltd*, above n 36.

155 Broadcasting Act 1989, s 2.

156 *Shetland Times Ltd v Wills* (1997) EMLR 277 (EWCA).

157 Ibid, 74 Hamilton LJ.

> … a service which consists wholly or mainly in sending visual images, sounds or other information by means of a telecommunications system, otherwise than by wireless telegraphy, for reception:
>
> (a) at two or more places (whether for simultaneous reception or at different times in response to requests by different users), or
>
> (b) for presentation to members of the public, and which is not, or so far as it is not, excepted by or under the following provisions of this section.

The BSA, in my view, chose an important element of distinction: the way of "consuming". Internet content is rarely accessed by accident, unlike television channels.[158] It can be called a pull-type medium, unlike television, which is more a push-type distribution of information.[159]

On the other hand, it is awkward that while radio and television are subject to stricter legal rules than printed press, the same content is not subject to the same rules if accessible through their internet websites. Nowadays it is almost common that traditional media actors have their corresponding websites on the internet.[160] The question is: is it reasonable that the same companies which provide the same content through different technological tools are subject to different regulations? Should TV programmes be treated differently if distributed through the internet than if through the traditional channels? Clarification of these questions and finding the place of ISPs in this system requires legislative response.

If we assume that the Broadcasting Act does not apply to internet content, then some traditional media actors may publish more risky content on the internet than through the original medium, developing a small gap between the content of the two platforms. They may have an interest in doing so, because the legal requirements of broadcasing are stricter worldwide than for content published in another manner, for example in the printed press.[161] Publication on the internet is generally thought to be even more liberal than printed press because not even registration is needed. Already some newspapers publish the politically harsher articles in their online version only, rather than on paper.[162] Broadcasters may choose to publish online those episodes or situations on a reality show which they would not show on television, or if they would, it would result in penalties.[163]

---

158 *ACLU v Reno (No 1)* (1996) 929 F Supp 824 para 88 (3d Cir) Sloviter J.

159 Lessig, above n 40.

160 See www.nzherald.co.nz, www.tvnz.co.nz.

161 See Barendt, above n 37; *Red Lion Broadcasting Co v FCC*, above n 38; *FCC v Pacifica Foundation*, above n 39).

162 For example the market leading Hungarian daily newspaper, Nepszabadsag.

163 As one of the biggest Hungarian commercial channels, TV2 used to do during a popular reality show titled "Big Brother".

However, applying broadcasting standards to internet content would raise even more unanswered questions. Beyond established television and radio programme providers, there are some content providers which publish their programmes online only; for example webradios are widely known. It would be also difficult to distinguish in legal terms between an amateur video and audio content from commercial broadcasting. Finally, this interpretation puts ISPs in danger of being regarded as broadcasters, especially in cases where the content provider is unknown.

For the purposes of this study I assume that broadcasting does not include online publication and I will use the term broadcaster only for the traditional broadcasters like television and radio.

2 Thoughts about the regulation of webcasting

If the situation is to be changed by legislation, there are different possibilities:

(a) To impose the same obligations on online audio and video content as on broadcasters;

(b) to deregulate television and radio; and

(c) to develop a new structure of regulation, using a new factor for differentiation between various types of content.

First, if the same obligations are imposed the already well-known difficulties of law enforcement would be minimised because the broadcaster companies typically have their businesses and assets within the country where they operate and penalties can be used against them if they do not follow the rules. For the same reason, it is expected that their content would not be significantly objectionable compared to other internet content. Of course, foreign sources which are not reached by domestic legislation are still accessible.

By including all online audio and video content under broadcasting, traditional broadcasting companies' online content would be covered satisfactorily. However, this goal could be achieved by less burdensome tools as well. The weakness of this solution is caused partly the existence of online-only media. There is no theoretical justification for restricting freedom of expression in the online arena, because the main traditional reasons have been largely eliminated by technological development.

Although the uniquely pervasive effect of the medium has not changed, there are significant differences in the way the medium is used. The psychological impact of the moving picture and sound is still stronger than that of written text, but both can be transmitted through the internet now. However, the internet is a pull medium and not a push medium, unlike traditional broadcasting.[164]

The rationale of spectrum scarcity has clearly weakened. Instead of scarcity we speak more about the abundance of information resources. One unbalanced website on its own is unlikely to

164 Lessig, above n 40.

influence the users and distort their views. The vast information overload that is characteristic of today's communication environment makes every piece of information relative to another piece of information. Even if a single website is viewed by millions of people a day, and has a huge impact, the existence of other, equally accessible information sources may mitigate its effect. Users have the choice to compare various sources. However, user behaviour does not necessarily follow this ideal news-consumption path. Users tend to read the same few favourite websites and do not enquire beyond those. Readers prefer media content which reassures them in their prior beliefs and opinions.[165] However, this observation ignores that the case has been the same with newspapers and television channels: people tend to buy only the newspaper which imparts views sympathetic to them. In fact, the internet has a good chance to improve this situation by making it easier to compare various sources. Whereas newspaper readers are very unlikely to buy the paper of an opposing political opinion, it demands less effort and investment to click on the website of the opposing newspaper just to compare their news coverage.

The acceleration of information flow sometimes means that biased information may spread quickly. But at the same time, the information may spread equally quickly whether the source is trustworthy or not.

Finally, a new legal rule regulating online media could conflict with section 14 of the BORA. Freedom of expression can be restricted only by "reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society."[166] However, according to section 7, this would not necessarily stop such rules from being passed.[167] It would be difficult to differentiate between amateur video and audio content and commercial media. Applying broadcasting standards to the internet would be an unacceptable restriction of freedom of expression and of receiving information. However, BORA's requirement for balancing and a proportionate restriction makes it highly unlikely that a court would interpret the existing content restrictions (which apply now to broadcasters), so as to apply to an average user who publishes her private video clip on the internet.[168]

Second, deregulation is worth considering as the "traditional" means of broadcasting has changed in such a dramatic way, so as to justify a complete reform of broadcast regulation. Spectrum scarcity has lost its relevance already through the appearance of cable and satellite television. Digital television might change the push feature of distribution by the pay-per-view system and interactive television use. If transmission of TV programmes through the TV-set and through the internet have to be harmonised, *deregulation* should be considered instead of more

---

165 Cass R Sunstein *Republic.com* (Princeton University Press, Oxford, 2001).

166 Bill of Rights Act 1990, s 5.

167 Ibid, ss 4-7.

168 Ibid, s 6.

regulation. This would create a technology-neutral legal environment, where all media would be subject to similar rules as newspapers.

Third, taking a new approach may be optimal. There is a strong tendency towards convergence: TV is watched through the internet, telephone calls are made through the internet, while internet is used through the mobile, and so forth. Differentiating between technological platforms is apparently not a good basis for regulation.

I would like to point to a parallel process which has been progressing for the past two decades. The number of ordinary users communicating interactively has exploded; they publish text, pictures, sounds and movies. At the same time the number of media and telecommunications companies is decreasing because of mergers (and convergence). This means that two big groups of communicators (publishers) are present in the media: the millions of amateurs and the few but very influential professionals.[169] One group is powerful because of the sheer number of its actors, and the other because of its financial power, transnational nature, and presence in more media branches. Most professional websites are regularly visited by masses, while amateur websites are seen usually only by a handful of friends and relatives. Of course, the internet makes shifting from an amateur to a professional publisher very easy and prompt. Still, professional publishers cannot survive if they do not make enough impact to finance their activities. Amateur sites can occasionally exercise enough impact to upgrade to professional.

However, it is still questionable what should be the criteria in deciding whether a site is professional or not. Various factors could be taken into consideration. One of them could be whether the site aims at yielding profit or not, another could be the regularity of the updating process. Under all circumstances, the distinction between professional publishing and simple user participation will not be easy to draw.

E Conclusion

Whether an ISP can be made liable or not depends on the definitions of words in existing legal rules such as "publication", "publisher", "agency", "broadcaster", and on the threshold of liability. Where the liability requires intentional action, ISPs are in no danger: they cannot be made liable unless they commit something illegal intentionally. Where negligence can entail liability, it depends on how courts interpret ISPs' obligations. Should they be expected to monitor content, they can easily fall short of fulfilling their obligations. Where the threshold of liability is strict or absolute, ISPs can be in danger of being made liable for something that they have not committed themselves. This is the area which requires attention either by courts or by legislation.

In absence of specific rules, ISPs must be aware of those illegal activities that might become relevant for them. However, there is not much they can do about these; because of the nature and

---

169 See also Ben H Bagdikan *The New Media Monopoly* (Beacon Press, Boston, 2004) 7, 25.

volume of internet communication, they are unable to prevent the emergence of certain illegal deeds, such as publication of objectionable material by one of their users. In addition, the present legal environment makes them unwilling to exercise increased awareness and undertake measures for protection against illegal material, because that could raise the threshold of liability. By getting more involved with others' content, they increase their awareness, and lose the defence of "innocent dissemination", or simply the position of the outsider who had no idea about the illegal content.

They can minimise their involvement by denying services to the user who uses their services to commit illegal actions. However, it is not always easy to decide whether an action is illegal, for example in cases of defamation, hate speech or privacy, because of the complexity of these offences. Therefore ISPs, in the absence of a statutory protection might overreact to such events, which will have a chilling effect on internet communication.

My hypothesis is that ISPs should be explicitly exempted from liability for content provided by third parties, whether they provide access, hosting, caching or searching services, or any other intermediary services invented in the future. Without such a general declaration, ISPs face a constant risk for any illegal activity committed by their customers or users. Some exceptions to the rule may be maintained, if it is regarded as necessary by the policymakers. The options and alternatives to the extent and the formulation of such exceptions will be detailed at the end of this study. Instead of the painstakingly detailed amendment of all the relevant Acts, introducing a general clause may be more efficient and may even better serve the purpose. In those areas where ISPs are meant to owe somewhat more responsibility, for example the area of copyright, specific provisions could be enacted in the relevant act.

VI INTERNATIONAL COMPARISON: SOME EXAMPLES OF ISP LIABILITY REGULATIONS IN CERTAIN COUNTRIES

A Australia

1 The notice-classify-takedown regime under schedule 5 of the Australian Broadcasting Services Act

The Australian legislation chose to expand the existing regulation of broadcast content and the regime of classification to internet content. This happened by way of an amendment to the Australian Broadcasting Services Act (ABSA) in 1999, targeting online services.

2 Co-regulation

The regime aims to achieve a co-regulatory scheme, where industry self-regulation completes legal regulation. The Act has some provisions which are to be applied only if there is no industry self-regulation. It also prescribes what needs to be addressed in the industry codes.[170] Both content

---

170 Broadcasting Services Act 1992 (Cth), Schedule 5 Part 5 Division 3 s 60(1-2) [Schedule 5].

providers and service providers are expected to develop codes.[171] If the code fulfils the requirements, the Australian Communication and Media Authority (ACMA) registers it.[172] It may request that a particular section of the internet industry develops a separate industry code.[173] The ACMA may also direct a participant of the relevant internet industry to comply with the industry code and may issue a formal warning.[174] It also has the right to determine industry standards itself in some cases if the ACMA is not satisfied with the code, or in the case of a partial or "total failure" of industry codes.[175] The ACMA holds strong powers in this co-regulatory regime, but the Act lists ample safeguards which prevent an arbitrary use of this power.[176]

The ACMA is entitled to issue online provider determinations, which are "written determination[s] setting out rules that apply to Internet service providers in relation to the supply of Internet carriage services", and similar determinations relating to internet content providers respectively.[177]

Also, the Act suspends the effect of possible State or Territorial laws as far as they make ISPs liable for hosting or carrying content that they were not aware of, or oblige ISPs to monitor, make inquiries of or keep records of content hosted or carried.[178]

The Act exempts providers from possible civil suits if they acted in compliance with the industry code, the industry standards or the Act's directions to remove or prevent access to content.[179]

3 Other functions of the ACMA

The ACMA has further functions related to community awareness raising, such as to advise and assist parents, co-ordinate community education programs, and liaise with regulatory and other relevant bodies overseas about co-operative arrangements for the regulation of the Internet industry.

The ACMA also may designate certain filters as approved restricted access systems for the purposes of the Schedule.

---

171 Ibid, s 59(1-2).

172 Ibid, s 62.

173 Ibid, s 63.

174 Ibid, ss 66-67.

175 Ibid, ss 68-71.

176 Ibid, ss 68(3), 69(1)(b), 70(1)c,(2)(4)(7), 71(1)d, (2)(4), 76-77.

177 Ibid, Part 6, s 80(1-2).

178 Ibid, Part 9, s 91.

179 Ibid, Part 8, s 88.

4 Dealing with prohibited content and potential prohibited content

Schedule 5 deals only with the last two categories of classified content: those rated RC or X18+ by the Classification Board. Content is prohibited if it has been classified as one of these classes, and in case it is hosted in Australia, an additional criterion is that access to it is not restricted. Potential prohibited content is content that has not been classified by the Classification Board, but should it be classified, it would probably be prohibited content.[180]

Films and videogames, if hosted on the internet in their entirety, retain their original classification. If they have not been classified, they can be classified by the Classification Board as they would be classified under the *Classification (Publications, Films and Computer Games) Act 1995*.[181]

5 How to make a complaint

Complaints may be filed if someone has encountered prohibited or potential prohibited content in Australia. A complaint can also be made through the online form at the ACMA's webpage.[182] If submitted in another form, it should at least contain the following elements:[183]

(a) identify the Internet content; and

(b) set out how to access the Internet content (for example: set out a URL, a password, or the name of a newsgroup); and

(c) if the complainant knows the country or countries in which the Internet content is hosted—set out the name of that country or those countries; and

(d) set out the complainant's reasons for believing that the Internet content is prohibited content or potential prohibited content; and

(e) set out such other information (if any) as the ACMA requires.

The complaint needs to be in writing,[184] but the complainant does not need to give her name or address. However, only persons resident in Australia or corporate entities carrying on activities in Australia may complain.[185] The online forms specify further details.[186]

---

180 Ibid, Part 3 Division 1, ss 10-11.

181 Ibid, Part 3 Division 1, s 12.

182 www.acma.gov.au.

183 Schedule 5 above n 170, Part 4 Division 1 s 22(3).

184 Ibid, Part 4, Division 1 s 24.

185 Ibid, Part 4, Division 1, s 25 – as well as the Commonwealth, a State or a Territory.

6 The procedure that follows the complaint

If the ACMA finds that the content complained of is prohibited content and is hosted in Australia, it issues a final take-down notice directing the ISP not to host the prohibited content. If the ACMA finds that the content hosted in Australia is potentially prohibited content, it issues an interim take-down notice, which directs the ISP not to host the prohibited content, and requests the Classification Board to classify the content. If the ACMA finds that if the content were to be classified there is a substantial likelihood that it would be classified as R18+ (rather than X18+ or RC), it requests the Classification Board to classify the content without issuing an interim takedown notice. If the Classification Board classified a particular content as prohibited content, the ACMA issues the final takedown notice.[187]

If the ISP complies with the interim take-down notice and gives the ACMA a written undertaking not to host the internet content before the Classification Board would classify the content in question, the ACMA gives notice to the Classification Board that classification is not necessary and revokes the interim take-down notice.[188] If ACMA finds out that content that has once been subject to an interim or final take-down notice is hosted in Australia, or content that is substantially similar to that, it may order the ISP to remove the content by a special take-down notice.[189] This targets mainly mirror sites and cache copies. ISPs must comply with the take-down notices not later than by 6 pm on the next business day.[190]

7 Internet content hosted outside Australia

If the internet content complained of is prohibited or potential prohibited content, but it is hosted outside Australia, the ACMA reacts differently. If the content is of a sufficiently serious nature, the ACMA notifies the Australian police force. The Act gives priority to the industry code (or industry standard) in such case, and provides for only a situation if there should be no industry standard: in this case ACMA notifies all known ISPs, issuing a standard access-prevention notice, which directs providers to do all reasonable steps to prevent end-users from accessing the content.[191] This would be actual blocking of foreign content, which is often despised in democratic countries. However, the latter provision does not need to apply, because the industry Code of Practice deals with the

---

186 See the online forms at: http://www.aba.gov.au/what/online/www.asp; there are three separate forms for online content in general, for newsgroup postings and for P2P content: http://www.aba.gov.au/what/online/newsgroup.asp; http://www.aba.gov.au/what/online/other.asp.

187 Schedule 5 above n 170, Part 4, Division 3, s 30(1-2)(4).

188 Ibid, Part 4, Division 3, s 33.

189 Ibid, Part 4, Division 3, s 36.

190 Ibid, Part 4, Division 3, s 37(1-2-3).

191 Ibid, Part 4, Division 4, s 40.

situation. It provides for a designated notification scheme which means that ACMA notifies the suppliers of the approved family friendly filters about the prohibited content and where it is hosted. The suppliers have undertaken to add such content to their list of prohibited content.[192] The ISPs (who also receive notification of such content from the ACMA[193]) have undertaken to make available approved family friendly filters to their clients at the cost of obtaining, supplying and supporting the filter.[194] The ISPs' obligations extend to making the filter easily downloadable or attainable by post, and to send information to their clients about the filters every four months.[195]

The Codes of Practice also list the requirements for approval of filters. Beyond being proven as effective, easy to install, easy to use, and so forth, the supplier of the filter has to agree that they will include the pages sent to them by the ACMA.[196] Suppliers have to submit their product to the Internet Industry Association regularly for testing of its appropriateness.[197] In fact, service provider industry codes must deal with this question, according to Part 5, Division 3, 60(2)d of the Act. One possible way to deal with this is highlighted in the Act: industry codes may declare designated alternative access-prevention arrangements, in which case an ISP is not required to deal with internet content outside of Australia. The Act recommends that such arrangements are, for example, regularly updated internet content filtering softwares, or family-friendly, filtered internet access service.[198] The ACMA may also declare some arrangements as recognised alternative access-prevention arrangements. (In absence of an industry-code regulation, those ISPs which offer such filters to their clients are not required to block access to prohibited, or potential prohibited content hosted outside Australia.[199])

Having the industry code providing for this situation, the ACMA notifies the ISPs about the content as set out in the code, so that the ISPs can add the site to the list of prohibited sites in their filtering softwares.[200]

The ACMA sends the complaint to the classification Board which then sends the classification back. This takes generally about one week and costs approximately AUD 510. The ACMA receives

---

192 Internet Industry Codes of Practice, Content Code 3, 19.2.(a) [IIC].

193 Ibid, Content Code 3, 19.2(b).

194 Ibid, Content Code 3, 19.3-4.

195 Ibid, Content Code 3, 19. 5-6.

196 Ibid, Schedule 1, 1-3.

197 Ibid, Schedule 1, 2.

198 Schedule 5 above n 170, Part 5, Divison 4, s 60(3)(6).

199 Ibid, Part 4, Division 4, s 40(4-5).

200 Ibid, Part 4, Division 4, s 40(1)b.

about 1000 complaints per year, about 75% of which are valid. From that about 600 are prohibited, but only about 3% of the prohibited content is hosted in Australia and the rest is hosted overseas.

8 Offences and penalties

Compliance with the take-down notices and the access-prevention notices is compulsory. Complying with these within the given time (6pm the next business day) is called an online provider rule, along with ACMA's directions to comply with the industry code,[201] compliance with the industry standards[202] and online provider determinations.[203] It is an offence to contravene these rules, and the penalty is 50 penalty units, which was AUD 5500 per day for an individual and up to 27,500 per day for a corporation in August 2006. However, a fine is imposed only by court and only as a last resort – it has not happened as at the above date. In a case of non-compliance, the ACMA first issues a formal warning.[204] If this is without heed, the ACMA may request the Federal Court to order that the person cease supplying the internet carriage service or hosting the content.[205] The ACMA also may give the providers a written direction, requiring that they take specific actions so as to comply with the rule, such as to implement an effective administrative system for monitoring compliance.[206] Contravening the direction is an offence as well.[207]

ACMA decisions may be reviewed by the Administrative Appeals Tribunal (AAT) on the request of the service provider affected.[208]

The Internet Industry Codes of Practice impose a further obligation on ISPs to report to ACMA if they become aware that another ISP hosts – or provides access to, respectively –prohibited content in Australia, as well as to inform the provider in question.[209]

9 Child pornography

The Criminal Code Act 1995 of Australia has been modified in 2004 so as to include a specific part about Telecommunications Offences. It imposes an explicit obligation on ISPs to report child

---

201 Ibid, Part 5 s 66(2).

202 Ibid, Part 5 s 72.

203 Ibid, Part 6, s 79.

204 Ibid, Part 6, s 84.

205 Ibid, Part 6, s 85.

206 Ibid, Part 6, s 83(2-3).

207 Ibid, Part 6, s 83(4).

208 Ibid, Part 10, s 92.

209 IIC above n 192, Content Code 1, 9., Content Code 2, 13.

pornography or child misuse material to the Australian Federal Police within a reasonable time. If they fail to do so, they are liable for up to 100 penalty units.[210]

Among others, this amendment makes it an offence *to access* material that contains child pornography.[211] By this, the Act clarifies the often controversial court practice of holding that the act of viewing child pornography, but not saving it, qualifies as "possession" for the purposes of criminal law. If the policy intention is to make those who view child pornography online but do not keep it liable for an offence related to child pornography, it is a better idea to express this policy and make law enforcement predictable.

Making ISPs liable for reporting child pornography is a good way of dealing with this socially harmful material. Opponents of the idea to exempt ISPs from liability unconditionally often argue that such exemption would make ISPs not interested in cooperating with the law enforcement. As we can see, there are other ways to make them interested. Imposing an administrative liability on ISPs to deal with child pornography addresses the problem of this socially harmful material while not placing a disproportionate burden on them (as being liable for the material would be).

10 Copyright

The Copyright Act 1968 of Australia has been amended by the Free Trade Agreement (FTA) Implementation Act in 2004. In fact, the amendment of 2000 already provided for exemption from liability for ISPs (carriage service providers), saying that they are "not taken to have authorised any infringement of copyright in an audio-visual item merely because another person uses the facilities so provided."[212]

However, the FTA Implementation Act provided for a far more comprehensive conditional exemption, obviously influenced by the Digital Millenium Copyright Act of the United States.[213] The FTA Implementation Act added Division 2AA to Part V of the Copyright Act 1968. It made four categories for the providers of access, caching, hosting, and searching services. Division 2AA defines the conditions of exemption in detail, and exempts ISPs from monitoring, and from the onus of proving the lack of awareness.[214]

---

210 Criminal Code Act 1995 (Cth), Division 474 Telecommunications offences, Subdivision C Offences related to use of telecommunications, s 474.19. [Criminal Code]

211 Ibid, s 474.19.(1)(a)(i).

212 Copyright Amendment (Digital Agenda) Act 2000 (Cth), s39B, s 112E.

213 17 USCA 512, see below in more detail.

214 Copyright Act 1968 (Cth), Part V Div2AA, 116AG (3-4), 116AH, 116AH(1)4-5, (2), 116AI [Copyright Act].

Courts may order access providers to disable access to certain content, or to terminate a specified account; they may order providers of hosting, caching and searching services to remove or disable access, to terminate a specified account, or to issue "[an]other, less burdensome, but comparatively effective order".[215] All ISPs must adopt and reasonably implement a policy that allows them to terminate the account of repeat infringers. Also, they must respect existing codes that provide for respecting standard technical measures used to protect and identify copyright material.[216] The expectations of ISPs are very similar to those in the DMCA: hosting and searching providers must remove or disable access to the material if they receive a notice, and also if they become aware of the infringement, or facts that make the infringement likely or apparent (even in absence of a notification).[217] The cache must be removed or access to it disabled only upon notification.[218] The Act mentions "notice … in a prescribed form" but does not define what the prescribed form is like or who defines it.[219]

The division sets the additional requirement that no financial benefit is directly attributable to the infringing activity. To define whether the benefit is directly related to the infringing activity, the courts must have regard to the charging practices of the industry and whether the benefit was greater than the usual benefit. In *UMA v Cooper*, the ISP tried to use the FTA Implementation Act as a defence.[220] It came into effect only after the first hearing of the trial, but the court held that even if it had been in effect already, it would not have exempted the ISP from liability.[221] Under the FTA Implementation Act the ISP should have adopted a policy to terminate the account of repeat infringers.[222] Further, the ISP ought not to have enjoyed an extra benefit of a commercial nature from hosting the infringing website.[223]

Beyond the similarities, there are significant differences to the DMCA. The Copyright Act 1968 does not provide for the form of notice, as mentioned above; it does not narrow the scope of complainants to the person harmed by the infringement or authorised by that person; it does not provide for replacing the material in case of a counter notice; it does not exclude ISPs' liability against the content provider; and it does not oblige ISPs to reveal the user's identity at all.

---

215 Ibid, Part V Div2AA, 116AG (3-4).

216 Ibid, Part V, Division 2AA, Subdivision D, 116AH (2)1.

217 Ibid, Part V, Division 2AA, Subdivision D, 116AH (1)4.2A, 5.2A.

218 Ibid, Part V, Division 2AA, Subdivision D, 116AH (1)3.3.

219 Ibid, Part V, Division 2AA, Subdivision D, 116AH (1)3.3.

220 *UMA v Cooper*, above n 11.

221 Ibid, 103-107 Tamberlin J.

222 Ibid, 107 Tamberlin J.

223 Ibid, 108, 115-117 Tamberlin J.

11 Defamation

In 2005 a unified Defamation Act had been passed in almost all states of Australia, except Western Australia and the Australian Capital Territory.[224] The Act, which became effective in the first half of the year 2006, establishes innocent dissemination as a defence.[225] The section gives a detailed description of who may count as "not the first or primary distributor", and among others these include:[226]

> (f) (ii) the operation of, or the provision of any equipment, system or service, by means of which the matter is retrieved, copied, distributed or made available in electronic form; or
>
> (g) an operator of, or a provider of access to, a communications system by means of which the matter is transmitted, or made available, by another person over whom the operator or provider has no effective control.

This appears to effectively exempt ISPs from liability for defamation as they act as intermediaries.

B Canada

1 Copyright Act 1985

Canadian copyright law exempted intermediaries from liability by defining the word "communication" so that it does not include transmission through the internet in 1997:[227]

> For the purposes of communication to the public by telecommunication,
>
> (...)
>
> (b) a person whose only act in respect of the communication of a work or other subject-matter to the public consists of providing the means of telecommunication necessary for another person to so communicate the work or other subject-matter does not communicate that work or other subject-matter to the public;

This section has been interpreted by court in the case *SOCAN v CAIP*[228] where the Federal Court of Appeal of Canada made it absolutely clear that ISPs are exempted from copyright liability, with the usual condition of having no actual knowledge about the matter. The Society of

---

224 The latter has retained its Defamation Act 2001 – which does not have an explicit innocent dissemination defence.

225 Defamation Act 2005 (Vic), s 32.

226 Ibid, s 32(f-g).

227 Copyright Act RSC 1985, c. C-42, 2.4(1)b [Copyright Act].

228 *SOCAN v CAIP* (2004) CarswellNat 1919.

Composers, Authors & Music Publishers of Canada (SOCAN) proposed a tariff which was to be paid by ISPs so as to compensate for enabling music pirating through their services. The tariff was filed to the Copyright Board, which held that ISPs do not perform "communication" under the Copyright Act[229] as their typical activity (including caching and mirroring).[230] SOCAN appealed and the court at first instance held that an "internet service provider creating a cache of internet material is a communicator and a participant in the copyright infringement."[231] Both the Canadian Association of Internet Providers (CAIP) and SOCAN appealed against this decision. The Court of Appeal changed the Board's opinion on jurisdictional questions, and also the decision of the lower court in saying that caching and mirroring are not to be taken as communication either. It examined the wording of section 2.4(1)b, and found that the word "necessary" refers to means that are reasonably useful and proper to achieve the benefits of enhanced economy and efficiency.[232] The Court added:[233]

> As long as an internet intermediary does not itself engage in acts relating to the content of the communication, but merely provides "a conduit" for information provided by others, it is protected. The characteristics of a conduit include a lack of actual knowledge of the infringing contents, and the impracticality of monitoring the vast amount of material moving through the internet.

Practically, the court interpreted the Copyright Act as very similar to the take-down notice systems of the United States and of the European Union.[234] As well:

> I would point out that copyright liability may well attach if the activities of the Internet Service Provider cease to be content neutral, e.g. if it has notice that a content provider has posted infringing material on its system and fails to take remedial action.

It also said it "agree[s] that notice of infringing content, and a failure to respond by 'taking it down' may in some circumstances lead to a finding of 'authorization'."[235]

2 Other Acts

The Criminal Code was amended in 2001 by the Antiterrorism Act, addressing, among others, online crimes.[236] It provides that upon an interim, and later, final court order, child pornographic

---

229 Copyright Act, above n 138.

230 *SOCAN* above n 228, 3.

231 *SOCAN*, above n 228.

232 Ibid, 4. The lower court held that caching was not absolutely necessary for internet communication, hence it should be excluded from s 2.4(1)b.

233 Ibid.

234 Ibid, 124.

235 Ibid, 127.

material shall be removed, a copy of it handed to the court, and the identification information of the content provider given.[237] The court may order that the content provider is notified; she may appear in court to show her reasons why the material should not be deleted.[238] Interestingly, if the content provider cannot be identified or located, or resides outside Canada, the ISP should post the text of the notice to the online location where the child pornographic material had been stored, until the time available for appearance.[239] If the court is satisfied that the material really is child pornography, it may order it be deleted, including the court's copy.[240]

The Canadian Human Rights Act (CHRA) extended the crime of communicating hate messages through telephone so that it includes communication through the internet as well.[241] But, at the same time, it exempted "owners or operators of a telecommunication undertaking" from liability, by stating that its facilities are used for transmission not communication.[242]

Under sections 318 and 319 of the Criminal Code it is a crime to advocate genocide, publicly incite hatred, and so forth. ISPs have no specific obligation, but a judge has the authority to order the removal of hate propaganda from a computer system that is available to the public.[243] In an internationally known case, the Canadian Human Rights Tribunal ordered Ernst Zündel to cease and desist from publishing his hate site under section 13 of the CHRA. Since the site was hosted in the United States, the order could not be enforced.

Interestingly, the Telecommunications Act forbids ISPs to block access to content.[244] This was subject to challenge in the recent case of *Warman*. Warman is a person who used to denounce hate sites, whose authors were then prosecuted and one of them imprisoned. He was subsequently personally harrassed and threatened by foreign hate sites. He asked the Canadian Radio and Telecommunications Commission (CRTC) to allow that the ISPs voluntarily block the sites in question. CRTC has the power to order to block sites,[245] but it held it would be inappropriate to

---

236 Antiterrorism Act SC 2001 c 41

237 Criminal Code RSC 1985, c. C-46, s 164.1.1 [Criminal Code].

238 Ibid, s 164.1.2.

239 Ibid, s 164.1.2.

240 Ibid, s 164.1.5.

241 Canadian Human Rights Act, 13(2).

242 Ibid, 13(3).

243 Criminal Code above n 237, 320.1.

244 Telecommunications Act, s 36.

245 Ibid; except where the Commission approves otherwise, a Canadian carrier shall not control the content or influence the meaning or purpose of telecommunications carried by it for the public.

consider granting the interim order without first giving Internet carriers and other interested parties the opportunity to comment." [246]

Warman asked not that the CRTC block these sites, but that it exempt ISPs from the prohibition of voluntary blocking, in case they want to do so. The CRTC may have thought it must be a slippery slope and it is unsure that this is possible at all without an amendment of the law. The fierce international criticism because of the procedure against the Zündel site could also have had an influence.[247]

3 Self-regulation and the notice and notice system

This Canadian invention is a form of self-regulation between the Canadian Association of Internet Providers (CAIP), the Canadian Cable Television Association (CCTA), and the Canadian Recording Industry Association (CRIA). According to the agreement, the CRIA notifies the ISPs in writing about an alleged infringement of copyright by a customer of the relevant ISP; upon which the ISP notifies its customer in writing and also sends a written confirmation to CRIA that the notification has happened. According to anecdotal evidence, in 80-90% of the complaints the infringing activity is terminated voluntarily and there are few repeated complaints relating to the same material and the same user.[248] The CAIP submitted a proposal to the House of Commons Standing Committee on Canadian Heritage on amending the law to this effect:[249]

> ISPs could be required, upon receipt of a statutorily-defined notice from a copyright holder alleging copyright infringement by a site hosted by the ISP, to in turn provide a statutorily defined notice of the allegation to the party responsible for the alleged infringing site within a specified period of time.

The proposal reached the status of a bill in the House of Commons,[250] but then a motion of no-confidence was successfully filed in the Parliament, which resulted in new elections and a new government. The pending bills of the old government were set aside.[251]

The Bill provided that upon receiving a notice which fulfils the requirements, ISPs should forward it to the customer.[252] The ISP has a right to charge a fee for this "service", which is fixed by

---

246 CNews Law and Order "CRTC won't block hate sites" (25 August 2006).

247 See also Jane Bailey "Private Regulation and Public Policy: Toward Effective Restriction of Internet Hate Propaganda" (2003) 49 McGill LJ 59.

248 Canadian Association of Internet Providers (CAIP) "Re: 'Supporting Culture and Innovation: Report on the Provisions and Operation of the Copyright Act' – Review by the House of Commons Standing Committee on Canadian Heritage Position Paper" (15 September 2003) [CAIP Position Paper].

249 Ibid, 6.

250 Copyright Bill C-60 2005 [Bill C-60].

251 Drew Wilson "Bill C-60 and Bill C-74 Die" (30 November 2005) Slyck http://www.slyck.com/newsphp?story=1011.

the Minister.[253] The ISP is also obliged to keep identification data of the customer for six months from the date of the notice.[254] If an ISP fails to fulfil this obligation, it is liable for statutory damages defined by the court, which cannot be more than CD 5000 for failing to send the notice, and CD 10,000 for failing to retain the customer's identification data.[255] Actual knowledge establishes liability if it is knowledge of a court decision which finds that the stored material is infringing.[256]

The notice and notice system is definitely more able to deal with the new peer-to-peer technologies than the old notice-and-takedown systems, for the sole reason that in the case of peer-to-peer technologies there is nothing the ISP could remove; the content is hosted at the users' computers.[257] Not monitoring customers' use of their access services, ISPs are unable to identify if the customers use their internet access for lawful or unlawful purposes.

C United States

1 Antecedents: the distributors' liability

The United States was perhaps the first country that regulated ISP liability. The need for regulation was raised by a series of court cases. Before the legislation was passed, courts used the analogue of the distributors' liability to deal with ISPs' liability for content provided by third parties.[258] The distributors' liability is based on the obvious requirement which we can observe as a typical approach for ISP liability throughout the world: the question whether the ISP was aware of the unlawful content or not.[259] However, the question goes further: whether the ISP ought to have known about the content. The courts had never said that the ISP was obliged to monitor, but where the ISP stipulated it would itself monitor content, it became liable for not performing this voluntarily undertaken – although unrealistic – duty.[260] By their declaration, which served mainly

---

252 Bill C-60 above n 250, ss 40.1.(1)(a-g) and 40.2.(1)a.

253 Ibid, s 40.2.(2).

254 And if the claimant starts a lawsuit and gives the ISP notice of this, until one year after this second notice; Ibid, s 40.2.(1)b.

255 Ibid, s 40.2.(3).

256 Ibid, s 31.1.(5).

257 See also Department of Canadian Heritage Copyright Policy Branch *Government Statement on Proposals for Copyright Reform – Internet Service Provider Liability* (24 March 2005).

258 *Cubby*, above n 2; *Stratton Oakmont*, above n 2.

259 *Cubby*, above n 2, 140 Leisure J.

260 *Stratton Oakmont*, above n 2, 2 Ain J.

marketing purposes, they themselves excluded the liability of distributors and elevated the threshold of liability to the publishers' level:[261]

> PRODIGY has uniquely arrogated to itself the role of determining what is proper for its members to post and read on its bulletin boards. Based on the foregoing, this Court is compelled to conclude that for the purposes of Plaintiffs' claims in this action, PRODIGY is a publisher rather than a distributor.

As a result, the court found Prodigy liable for a bulletin board posting which contained defamatory comments.[262] The comments did not use abusive language, therefore they were not automatically filtered out. The ISP did not receive a notice to remove the content before being sued.[263] This decision is often mentioned as the trigger for the legislation about ISPs. In fact, the legislation was already pending when the case was decided, and the court was aware of that:[264]

> In addition, the Court also notes that the issues addressed herein may ultimately be preempted by federal law if the Communications Decency Act of 1995, several versions of which are pending in Congress, is enacted.

However, the Act was not passed for some time and in the interim the Congress is reported to have discussed the Prodigy decision as one that had to be overruled.[265] The Communications Decency Act (CDA) (among other, less successful provisions)[266] exempted ISPs from liability in plain language: "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[267] For a couple of years this was acknowledged as an unconditional exemption from liability for third party content.[268] However, discussion arose around interpretation of the article.[269] The new interpretation

---

261 Ibid, 4 Ain J.

262 Ibid.

263 Or at least it is not mentioned in court.

264 *Stratton Oakmont v Prodigy*, above n 2, 5 Ain J.

265 See *Barrett v Rosenthal* (2003) 5 Cal Rptr 3d 416, 435-436 Kline J; See also *Barrett v Rosenthal (No 2)* (2004) 9 Cal Rptr 3d 142.

266 *ACLU v Reno*, above n 64.

267 47 USCA §230(b-c).

268 See *Blumenthal v Drudge*, above n 2; *Zeran v America Online, Inc*, above n 2; see also Jonathan Zittrain "A History of Online Gatekeeping" 19 HVJLT 253, 263 ("the CDA's immunities were thought in early interpretive cases to be broad enough to preclude both publisher and distributor liability").

269 See Paul Ehrlich "Communications Decency Act § 230" (2002) 17 Berkeley TLJ 401; Susan Freiwald "Comparative Institutional Analysis in Cyberspace: The Case of Intermediary Liability for Defamation" (2001) 14 Harvard J Law & Tec 569; Sewali K Patel "Immunizing Internet Service Providers from Third Party Defamation Claims: How Far Should Courts Go?" (2002) 55 Vand LR 647.

was that Congress' intention had been to exempt ISPs from being liable as publishers, but not from the obligations of a distributor. This is how the CDA is currently construed.[270]

Interestingly, one of the arguments most often used against the unconditional exemption of §230 of the CDA is the Court of Appeals' decision and reasoning in the *Zeran* case.[271] The District Court of Virginia, and later the Fourth Circuit Court of Appeals did not award damages to Zeran against AOL which carried the anonymous defamatory messages on its bulletin board. Zeran argued that §230 exempted ISPs from being liable as a publisher, but not from being liable as a distributor. In fact the decision would not have been different under the distributors' liability because AOL promptly removed the messages after the notice, it only refused to publish a retraction.[272] No law or self-regulation has ever imposed the duty to publish a retraction on ISPs anywhere on the world. This would obviously contradict their role as intermediaries.

Zeran argued that AOL was liable as a distributor because it did not promptly remove the messages. In fact, according to the courts' records, AOL removed the first defaming message on the day after it appeared (26 April), and the 4 consecutive messages within the following five days, so that the last one was removed on the 1 May.[273] It would be difficult to argue that AOL was negligent – rather the defaming person was really too "diligent" by reposting the messages again and again.

The Court held that AOL was not liable, but for different reasons than those above: it held that the CDA provided an absolute immunity. In the Court's opinion, distributors' liability was only a subset of publishers' liability. In its interpretation, being a distributor meant that the person becomes liable as a publisher only after it acquired actual knowledge of the infringing material. According to this reasoning, even if the person acquired the actual knowledge, that person was not to be held to be a "publisher", therefore it did not have to do anything with it:[274]

> once a computer service provider receives notice of a potentially defamatory posting, it is thrust into the role of a traditional publisher. The computer service provider must decide whether to publish, edit, or withdraw the posting. In this respect, Zeran seeks to impose liability on AOL for assuming the role for which § 230 specifically proscribes liability--the publisher role.

In a later case, *Blumenthal v Drudge*, the Court used the same approach, although reluctantly, because in that specific situation the outcome seemed unjust. "Whether wisely or not, it made the

---

270 See for example *Grace v eBay* (2004) 16 Cal Rptr 3d 192, 199 Croskey J for the Court; *Barrett v Rosenthal*, above n 265.

271 *Zeran No 2*, above n 2.

272 *Zeran No 1*, above n 2, 1127-1128 Ellis J.

273 Ibid, 1129 Ellis J.

274 *Zeran No 2*, above n 2, 333 Wilkinson J.

legislative judgment to effectively immunize providers of interactive computer services from civil liability in tort with respect to material disseminated by them but created by others."[275]

The *Drudge* decision was followed by criticism of the CDA's interpretation. A new approach emerged, asserting that the CDA immunised ISPs only from publishers' liability, but not from distributors' liability.

There were some further controversial cases, where the courts extended the immunity to ISPs who actually *provided* content rather then only distributed it. In both the cases of *Batzel v Smith* and *Barrett v Rosenthal*, "distribution" of the content was based upon an informed choice.[276] In *Batzel*, the listserver distributed an email that was sent to him and not to the list. The sender of the email did not intend to have it spread through the list. This was distribution in the meaning of "spreading" the message, rather than distribution in the meaning of "conveying" the message automatically.[277] In *Barrett*, similarly, the participant in certain newsgroups posted certain information according to her choice and her convictions. "Rosenthal refused to withdraw the message and, on unspecified dates, posted 32 additional messages on specified Internet newsgroups describing appellants' threat accompanied by a copy of Bolen's allegedly defamatory message".[278] In my view this cannot be regarded as simply mediating messages, also considering that the defendant referred to "appellants as, among other things, 'quacks'".[279] Nevertheless, the courts treated these actors as "distributors" and blamed the *Zeran* decision for not making these defamers liable.

In fact, section 230 of the CDA provoked an unexpected reaction from many courts: the formulation that it protected the "good Samaritan" invited moral indignation when it had to be applied to ISPs which did not filter their content.[280]

> § 230(c) bears the title "Protection for 'Good Samaritan' blocking and screening of offensive material", [is] hardly an apt description if its principal effect is to induce ISPs to do nothing about the distribution of indecent and offensive materials via their services. Why should a law designed to eliminate ISPs' liability to the creators of offensive material end up defeating claims by the victims of tortious or criminal conduct?

---

275 *Blumenthal v Drudge*, above n 2, 50 Friedman J.

276 *Batzel v Smith* (2003) 333 F 3d 1031 (9th Cir); *Barrett v Rosenthal*, above n 265.

277 See also Jae Hong Lee "Batzel v Smith & Barrett v Rosenthal: Defamation Liability for Third-Party Content on the Internet" (2004) 19 Berkeley Tech L J 469, 5.

278 *Barrett v Rosenthal*, above n 265, 146 Kline J.

279 Ibid.

280 *Doe v GTE Corp* (2003) 347 F 3d 655, 660 (7th Cir).

The contrast created a general feeling of injustice and made courts reluctant to accept that section 230 protects ISPs also when they do not filter inappropriate material.[281] I cannot see any other reason why there has been such a strong opposition of *Zeran* even in cases where the facts were very different (for example in the case of *Batzel*).

Distributors' and publishers' liability are now regarded as two separate liability structures. The recent decisions already took it for granted that the CDA provides exemption only from publishers' liability, but not from distributors' obligations.[282] The *Zeran* court's interpretation is rebutted:[283]

> it ignores the fact that in the common law of libel the publisher/distributor distinction has existed for many years. While a distributor has similarities to a publisher, and is occasionally called a secondary publisher, the common law has always considered the categories of publisher and distributor as two separate categories subject to two independent types of liability. The common law created the distinction between a publisher and distributor based on the common sense policy that a publisher has a higher degree of involvement in the dissemination of defamatory material and should therefore be subject to a separate, higher standard of liability.

The argumentation is similar in *Barrett v Rosenthal*:[284]

> When distinguishing the liability of publishers and distributors, eminent law professors writing scholarly articles in learned journals commonly use the word "publisher" to refer only to a primary publisher, even when their subject is the transmission of speech in cyberspace.

The traditional distributor liability therefore is alive again in the United States, which practically makes ISPs liable for carrying or hosting content once they are aware of its unlawful nature. If they are notified about such, they are supposed to remove the content. The result is very close to the notice and takedown systems of the European Union.[285]

One important principle is missing from the explicit legal rules: that ISPs are not expected to filter or monitor content, but allowed to do so.

2 The Digital Millennium Copyright Act

The Act (DMCA) was passed in 1998 and was addressed to the challenges of new technology.

---

281 *Blumenthal v Drudge*, above n 2.

282 *Grace v eBay*, above n 270, 199 Croskey J for the Court; *Barrett v Rosenthal*, above n 265. See also Emily Fritts "Internet Libel and the Communications Decency Act: How the courts erroneously Interpreted Congressional Intent with Regard to Liability of Internet Service Providers" (2004-2005) 93 KYLJ 765.

283 Patel, above n 269, 681-682 (citations omitted).

284 *Barrett v Rosenthal*, above n 265, 433 Kline J.

285 E-Commerce Directive, above n 71.

It established a so-called safe harbour for ISPs, while providing for the "expedient" removal of allegedly copyright-infringing material.[286] This was the first to introduce explicitly the notice-and-takedown regime.

The Act limits the liability of ISPs when they provide access, cache, hosting or searching services, as well as nonprofit educational institutions when acting as service providers, relating to content infringing copyright.[287] In each case, it lists a number of conditions that shall be used to establish whether the ISP is entitled to the exemption.[288]

For caching, hosting and search tool providers it sets further requirements of how ISPs have to react when they encounter copyright infringing material.[289] For all service providers, an additional condition is that they adopt a policy which enables termination of repeat infringers' accounts.[290] Also, they have to respect the technical measures that copyright holders use to identify and protect copyrighted works.[291]

A caching provider has responsibilities if material has been previously removed from the originating site or access to it has been disabled, or a court has ordered that it be removed, and it receives a notification of claimed infringement (similar to the one that is to be sent to hosting providers) in which the party confirms these facts.[292] In such a case the caching provider has to remove the cache expediently.[293]

The most extensive regulation relates to ISPs that provide hosting services. The notice procedure is discussed in this part, and used as a reference point in other parts of the Act.[294] First of all, hosting providers must not have actual knowledge about the infringing nature of the material, or of facts or circumstances which would make infringing activity apparent,[295] must not receive a financial benefit directly attributable to the infringing activity,[296] and also must have a designated agent to receive notifications, whose name, address, phone number and electronic mail address are

---

286 17 USCA § 512 [DMCA].

287 DMCA, above n 286 (a)-(e).

288 Ibid, (a)(1-5); (b)(1)(A-C), (b)(2)(A-D); (c)(1)(A)i-ii, (c)(1)(C); (d)(1-2), (e)(1)(A-C).

289 Ibid, (b)(2)(E)(i-ii); (c)(1)(A)(iii), (c)(1)(C), (c)(2-3); (d)(3).

290 Ibid, (i)(1)(A).

291 Ibid, (i)(1)(B), (i)(2).

292 Ibid, (b)(2)(E)(i-ii).

293 Ibid, (b)(2)(E).

294 Ibid, (c)(3), referred to in (b)(2)(E), (d)(3), (e)(1)(B), (h)(2)(A), (h)(4-5).

295 Ibid, (c)(1)(A)(i-ii).

296 Ibid, (c)(1)(B).

given to the Copyright Office.[297] Upon obtaining knowledge, or receiving notification, a content host must expeditiously remove, or disable, access to the material.[298] The notification must be in writing and can be submitted only by a person who is authorised to act on behalf of the owner of the copyright.[299] It must contain certain compulsory elements, such as identification of the copyrighted work that is claimed to have been infringed, identification of the material that is claimed to be infringing, and contact information of the complaining party.[300] If the notice contains at least these three elements which are regarded as substantial, the ISP is obliged to contact the complainant and assist to complete the notice.[301]

Searching tool providers, too, must be unaware of the infringing nature of a material, or facts which would point to this, and not receive a financial benefit directly attributable to the infringing activity.[302] They can be notified similarly to content hosts and they have to remove the link accordingly.

State and other nonprofit universities are also exempted from liability for the acts of their users. This was necessary because thousands of students use university networks and often they were found to infringe copyright. Several defamation suits also targeted university service networks.[303] A university is exempted from liability for acts of its teachers or students, unless the activity involves the provision of instructional materials online which are or were required in the previous three years for a course, or the institution has received already more than two notifications during the previous three years against the same person.[304] An additional condition is that the institution provides to all users appropriate information about the copyright laws.[305]

The DMCA also provides for the replacement of the material upon request of the content provider.[306] First of all, the ISPs are exempted from liability for the act of removing the content provider's material, regardless of whether or not the material is finally found to be infringing.[307]

---

297 Ibid, (c)(2).

298 Ibid, (c)(1)(A)(iii), 17 U.S.C.A. § 512 (c)(1)(C).

299 Ibid, (c)(3)(A)(i).

300 Ibid, (c)(3)(A)(ii, iii, iv).

301 Ibid, (c)(3)(B)(ii).

302 Ibid, (d)(1)(A-B), (d)(2).

303 For example *Godfrey v University of Minnesota* 1997-G-No 1187, and *Godfrey v Cornell University* 1997-G-No 1188.

304 DMCA above n 286, (e)(A-B).

305 Ibid, (e) (C).

306 Ibid, (g).

307 Ibid, (g)(1).

However, to avail itself of this exemption, the ISP must follow the following procedure. First, it has to notify the content provider when the material is removed. The content provider has the right to request by way of a formal counternotice that her material is put back. The ISP then forwards this "counter notification" to the complainant, informing her that it will replace the removed content within 10 business days.[308] The complainant may prevent this by sending a notice to the ISP again, stating that she has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity.[309] If the complainant does not file a court procedure, the ISP has to replace the content within 14 days after the counternotice.[310]

It is questionable, why the initiation of an action need have an effect identical to an injunction. Ten days should be enough to achieve an injunction, if the complainant effectively wants to prevent the material getting uploaded again.

In addition, as discussed regarding the Canadian notice and notice regime, time is not a crucial factor in the case of copyright infringements. Compared to the notice and notice regime, the provisions of DMCA significantly favour the copyright holder to the detriment of both the content provider and the ISP. In addition, the content provider may request the put-back only with the argument that it had been removed by mistake or because of misrepresentation.[311]

In case the content provider is anonymous, the complainant will be interested in revealing their identity. This can be done by way of a subpoena that is also regulated in the DMCA. It does not specify which type of service provider is obliged to disclose user data upon a subpoena.[312] This was the main question to be resolved by court in *RIAA v Verizon.*[313] The complainant requested the identification of subscribers who infringed copyright using peer-to-peer technology.[314] Verizon refused to disclose the data, because it interpreted the Act so that it requires disclosure of data only from hosting providers, whereas Verizon, in this case, acted only as access provider.[315] It deduced this from section (h)(2)(A) which requires that "a copy of the notification described in subsection (c)(3)(A)" shall be attached to the subpoena. A notification according to section (c)(3)(A) can be sent only concerning content hosted by the ISP, and in this case there was no such content,

---

308 Ibid, (g)(2)(b).

309 Ibid, (g)(2)(c).

310 Ibid.

311 Ibid, (g)(3)(c).

312 Ibid, (h)(1).

313 *RIAA v Verizon (No 1)* (2003) 240 F Supp 2d 24 (D DC); *RIAA v Verizon (No 2)* (2003) 351 F 3d 1229 (DC Cir).

314 *RIAA v Verizon (No 1)*, above n 313, 28 Ginsburg J for the Court.

315 DMCA, above n 286 (a); *RIAA v Verizon (No 1)*, above n 313, 29 Ginsburg J for the Court.

consequently no such notice. This resulted, in Verizon's (and later the Court of Appeals') interpretation that the subpoena resulted from a formal mistake. Section (h)(2)(4) says that the subpoena can be issued only if it fulfils all mentioned requirements. The Court of Appeals accepted that – although the legislator could not have foreseen this kind of development of the peer-to-peer technology – the wording of the law does not make it possible to oblige Verizon to disclose the data of its subscribers.[316] "P2P software was not even a glimmer in anyone's eye when the DMCA was enacted", and "[i]t is not the province of the courts, however, to rewrite the DMCA in order to make it fit a new and unforeseen internet architecture."

It is to be noted that DMCA is very detailed, and is a leading authority on how to deal with illegal online material, and also serves as a guide for ISPs. However, its solutions are not apt to deal with the newest of new technologies: the rapidly spreading peer-to-peer applications.

3 Child pornography

The Criminal Code deals with general issues relating to child pornography at the federal level,[317] and there are state regulations as well. The federal legislation obliges ISPs to report child pornographic material "as soon as reasonably possible".[318] Failure to report, if it happened "knowingly and willfully", may result in a fine of not more than USD 50,000 in an initial case an not more than USD 100,000 in subsequent cases.[319] The law also exempts ISPs from the requirement of monitoring, and from any liability "on account of any action taken in good faith to comply with or pursuant to this section".[320]

Pennsylvania state law provides for removal by a court order, but a court order may be requested only by "the investigative or law enforcement officer that has [such powers] in the official scope of that officer's duties".[321]

The federal criminal provisions on child pornography contain the word "knowingly", thereby criminalising intentional distribution only:[322]

> (a) In general. Any person who, in a circumstance described in subsection (d), knowingly produces, distributes, receives, or possesses with intent to distribute, a visual depiction of any kind, including a drawing, cartoon, sculpture, or painting ...

---

316 *RIAA v Verizon (No 2)*, above n 313, 1239 Bates J.

317 18 USCS, §1466A.

318 42 USCA, §13032.

319 42 USCA, §13032(b)(4).

320 42 USCA, §13032(c).

321 PA ST 18 PaCSA, §7626(2). See also PA ST 18 PaCSA, §6312.

322 18 USCS, §1466A(a).

The Federal state law provides for a defence which is similar, but not equal, to the notice and takedown regime. This defence can benefit only a person who did not possess more than three child pornographic pictures:[323]

> (e) Affirmative defense. It shall be an affirmative defense to a charge of violating subsection (b) that the defendant--
>
> (1) possessed less than 3 such visual depictions; and
>
> (2) promptly and in good faith, and without retaining or allowing any person, other than a law enforcement agency, to access any such visual depiction--
>
> (A) took reasonable steps to destroy each such visual depiction; or
>
> (B) reported the matter to a law enforcement agency and afforded that agency access to each such visual depiction.

4 Self-regulation

The United States Internet Service Provider Association (USISPA) addresses the question of liability for internet content in its Founding Principles.[324] It declares:[325]

> As a general rule, liability for Internet content should rest with the creator or initiator of the illegal content and not with an entity that retransmits, hosts, stores, republishes, or receives such content.

It also retains the right to block or filter traffic, and to obtain "Good Samaritan" immunity from liability for such action.[326]

It further says that ISPs should accept responsibility for disabling access to hosted content, but only as it is prescribed by law, or by a court order.[327] It does not mention anything about notice submitted by anyone else, hence it does not encourage ISPs to react to notices from the civil society. It merely emphasises that ISPs retain the right to remove content voluntarily, (and refers to the Good Samaritan protection again as related to the use of this right); but does not say anything about fulfilling takedown requests in general. On the contrary, it says that ISPs' obligations to disable access to hosted content should – among others – be based upon a legal framework or court order establishing such obligation.[328]

---

323 18 USCS, §1466A(e).

324 USISPA Founding Principles.

325 Ibid, "Internet Content".

326 Ibid, para 2.

327 Ibid, para 3.

328 Ibid, para 4.

D The Regulation of the European Union, on the Example of the United Kingdom

1 Background

The European Union chose to settle ISP liability for third party content with the European E-commerce Directive.[329] Directives are legal instruments of harmonisation of the laws of the member states in the European Union. They cast a common framework of regulation which the member states can fill with content in detail. Directives set legislative goals and it is up to the member states how to achieve those goals within the given deadline. Implementation of the directive can take place through one or more new laws, or by amending old laws. The implementation of a directive must not result in a substantial difference from the other member states' implementation and interpretation of the directive.

As is usual with directives, the E-commerce Directive is very plain and sets only basic rules without going into detail. Many of the countries, including the UK, did not provide for many more detail in their implementation.[330]

The main goal of the E-commerce Directive was to set up a necessary legal environment for electronic businesses. Regulating ISPs' liability was just an additional by-product, rather than the main goal. This may be another reason why these provisions are not more detailed. The Directive clarified that ISPs do not need to monitor content, and introduced a distributor-like liability. Exempting ISPs from liability was inspired by a few court cases where they were held responsible for content.[331]

For example, in the already-classic German *Compuserve* case, the director of the ISP Compuserve Germany was arrested and removed from his office handcuffed when his ISP provided access to pornographic newsgroups in 1995.[332] This had been preceded by a search carried out at the premises of the ISP. The charges were that stories describing child pornography were being disseminated through the computer system of Compuserve USA. Upon request of Compuserve Germany, Compuserve USA blocked access to the paedophile newsgroups, however, it did not do so concerning the "normal" erotic ones, which are also illegal in Germany, and which also contained at least one paedophile picture. Later the police handed over a list of 282 newsgroups that were to be blocked, and Compuserve USA blocked these newsgroups accordingly for two months.[333] After that

---

329 E-Commerce Directive, above n 71, Articles 12-15.

330 And Hungary and Germany.

331 Rosa-Julia Barcelo "On-line Intermediary Liability Issues: Comparing EU and US Legal Frameworks" (2000) European Intellectual Property Review 22(3) 105, 106.

332 Blake Cooper "The US Libel Law Conundrum and the Necessity of Defensive Corporate Measures in Lessening International Internet Libel Liability" (2005) 21 ConnJIL 127, 146.

333 *Local Court Munich v Felix Somm* No: 8340 Ds 465 JS 173158/95 (Amtsgericht Munchen).

it lifted blocking but sent electronic letters to each of their customers, including those in Germany in German language, informing them about the possibility of filters, and provided them the filter CyberPatrol free of charge. They thought they had made all the effort that could reasonably be expected, but the court disagreed.[334] Somm was sentenced to two years of probation and a fine of DM100,000.[335] However, very soon an amendment in the Act was passed, and it allowed the prosecution to appeal in favour of Somm, who was acquitted in the appellate court.[336]

In 1998 the French courts found a website host liable on two instances, after anonymous renters of webspace published photograph of Estelle Hallyday which infringed her copyrights and privacy. The Court held that the ISP should have monitored and controlled the information stored on its server.[337] In another, American, case, the church of Scientology sued Netcom, an ISP, because it gave access to internet newsgroups containing allegedly copyright infringing material.[338]

2 The Directive and the Regulations

The directive is built to a great extent on the principles of the DMCA, but its provisions are far from the DMCA's particularity. (For example, while the DMCA (§ 512) is 4141 words, Section 4 of the Directive consists of only 720 words).

The United Kingdom implemented the Directive by passing the Electronic Commerce (EC Directive) Regulations 2002 (Regulations).[339] It transplants the original text of the Directive with minor changes. I will describe the Directive by describing the Regulations and highlighting the differences where there are any.

Perhaps the most special feature of the European regulation is that it opts for a horizontal approach; it addresses all sorts of criminal and civil liability in one legal instrument.[340] Its exemptions apply in all possible cases of illegal content, such as defamation, child pornography, copyright or hate speech (where prohibited).

---

334 Birnhack and Rowbottom "Shielding Children: the European Way" (2004) 79 Chi-Kent LR 175, 207; George Ivezaj "Child pornography on the Internet: an Examination of the International Communities Proposed Solutions for a Global Problem" (1999) 8 MSU-DCL JIL 819, 842-843; Richard Derham "Internet-Regulation – Online Service Providers' Liability for Material Sent Over their Networks" (1997) CTLR 3(5) T117-118, 117.

335 Ivezaj, above n 334, 842; Cooper, above n 186, 146.

336 Birnhack and Rowbottom, above n 334.

337 *Hallyday v Lacambre*, 1999 Cour d'Appel de Paris.

338 *Religious Technology Center v Netcom, Inc*, above n 133. The case ended with settlement.

339 Electronic Commerce (EC Directive) Regulations 2002 (UK) [UK Regulations].

340 Luca Tiberi and Michele Zamboni "Liability of Service Providers" (2003) CTLR 9(2) 49, 51.

The Directive and the Regulations differentiate between the access, caching, and hosting providers. Unlike the DMCA, they do not include search engines (or information location tools, which may be understood to include hyperlinking[341]). Some countries, like Austria, Spain, Portugal and Hungary have extended the exemptions to providers of hyperlinks, search engines and content aggregation.[342]

The British government has also examined the necessity of extending the exemptions on hyperlinking. The Department of Trade and Industry (DTI) published a Consultation Document on the liability of hyperlinkers, location tools and content aggregators in relation to the Electronic Commerce Directive on June 8 2005.[343] However, the DTI found that there was enough protection for these service providers in most cases. For example, they are covered by section 1 of the Defamation Act 1996 (see below) and by section 97(1) of the Copyright, Designs and Patents Act 1998. Their liability may arise when information that is in contempt of court is accessed in the UK through their services. But then, asked the DTI, why should they be exempted from liability, which arises from risks associated with pursuing their profitable activity?[344]

Also, it suggests that they probably would not be made liable, at least not in copyright cases, because the provision of a hyperlink to copyrighted material does not necessarily result in the person using the link and infringing copyright. Further, it concluded that anyone who posts information on the net must assume that others provide links to it and her consent is implied.[345] However, at least in one known case the court was of a different opinion. In the *Cooper* case the Federal Court of Australia not only held the content provider liable for providing links to copyrighted materials, but also the ISP.[346]

An access provider, a "mere conduit", is exempted from liability and does not have any obligations with respect to content if it:[347]

(a) did not initiate the transmission;

(b) did not select the receiver of the transmission; and

(c) did not select or modify the information contained in the transmission.

---

341 Victoria McEvedy "The DMCA and the E-Commerce Directive" (2002) EIPR 24(2) 65, 71; see also Tiberi and Zamboni, above n 341.

342 Rico Calleja "Limitations on Liability of Intermediaries – DTI Consultation" (2005) CTLR 11(7) 219, 219.

343 See http://www.dti.gov.uk/consultations/page13985.html.

344 Calleja, above n 342, 220.

345 Ibid, 220.

346 *UMA v Cooper*, above n 12.

347 UK Regulations, above 339, s 17(1).

Its activity may include automatic, intermediate and transient storage (not cache copies). Such storage should take place only for the purpose of carrying out the transmission, and only for a reasonably necessary time.[348]

The Regulations describe the exemption from liability in more detail than the Directive, detailing that the ISP shall not be liable for damages, or for any other pecuniary remedy, or for any criminal sanction.[349] The mere conduit is not liable even if it is aware of illegal material and fails to take steps to prevent communication.[350]

Caching is also defined exactly as in the Directive: automatic, intermediate and temporary storage which serves only to make transmission more efficient.[351] The ISP shall not be liable if it does not modify the information, complies with the conditions on access to the information, complies with the rules on updating the information, and does not interfere with the lawful use of technology.[352] In addition, it has the obligation to remove or disable access to the information expeditiously if it obtains actual knowledge that it has been removed from the network, or access to it has been disabled, or that a court or administrative authority has so ordered.[353]

Hosting providers are not liable for information if they have no actual knowledge of unlawful activity or information, and neither are they aware of information that would make unlawful information apparent. In addition, upon obtaining such knowledge they have to expediently remove or disable access to the information.[354] If the recipient of the service (the content provider) was acting under the control of the ISP, the latter cannot be exempted.[355]

For each type of service provider, the Regulations omitted (from the Directive) provisions that the exemptions do not affect "the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement",[356] but mentioned a very similar provision in section 20, retaining the right of any

---

348 Ibid, s 17(2), or E-Commerce Directive above n 71, Article 12.2.

349 UK Regulations, above 339, ss 17(1), 18(1), 19(1).

350 *Bunt v Tilley* [2006] EMLR 18, 538 Eady J, (QB) citing *Gatley on Libel and Slander* (10 ed, Sweet & Maxwell, London) para 6-18.

351 UK Regulations, above 339, s 18(a), or E-Commerce Directive, above n 71, Article 13(1).

352 UK Regulations, above 339, s 18(b) (i-iv).

353 Ibid, s 18(b)(v).

354 Ibid, s19(a), E-Commerce Directive, above n 71, Article 14.1.

355 UK Regulations, above 339, s 19(b), E-Commerce Directive, above n 71, Article 14.2.

356 E-Commerce Directive, above n 71, Articles 12.3, 13.2, 14.3.

party to apply to a court to prevent or stop infringement.[357] Subsection (2) repeats the Directive's provision relating to administrative authorities.

Important additions come at the end of the relevant provisions in sections 21 and 22. First, the burden of the proof is expressly removed from ISPs:[358]

> Where evidence is adduced which is sufficient to raise an issue with respect to that defence, the court or jury shall assume that the defence is satisfied unless the prosecution proves beyond reasonable doubt that it is not.

This is in accordance with the Directive's meaning, but creates an additional legal certainty.[359]

Also, Regulation 22 provides how actual knowledge shall be established. It mentions notice and sets some criteria beyond the general guidance that courts shall take into consideration all matters which may appear relevant. The wording of the section is still rather soft, leaving it to the courts to decide whether a certain notice is sufficient to establish actual knowledge. The criteria only include giving the contact information of the complainant, the location of the material and in what way is it unlawful.

The Regulations omit one important statement from the Directive: that ISPs have no obligation to monitor content. This is the core of the Directive, upon which the whole structure of exemptions is built. It is essential to set the level of their duty. It would not be enough to declare that ISPs are not liable for illegal content that they are unaware of, if they could be made liable for being unaware. This happened in the American *Prodigy* case: although Prodigy did not know about the defaming content, the court found that they should have known about it. But, on the one hand, Prodigy held itself out as filtering content and this served as a basis for the court's findings. On the other hand, the *Prodigy* decision is generally held to be a less successful one. Hopefully this omission does not have any practical effect in the UK. In such cases the European Directive also serves as a back-up, as it can be referred to in any national court.[360]

3 Differences between the Directive (or the Regulations) and the DMCA

One of the most conspicuous differences is the lack of particular regulation of the notice procedure.[361] Although the Regulations outline some criteria[362] it is still far from the painstakingly

---

357 UK Regulations, above 339, s 20(1)(b).

358 Ibid, s 21(2).

359 A similar provision is in the Australian Copyright Act, above n 214, 116AI Division 2AA.

360 The legal sources of the European Union have a direct effect. Directives have a direct effect after their deadline for implementation: *Grad v Finanzamt Traunstein* (Case 9/70) [1970] ECR 825.

361 See also McEvedy, above n 341, 72.

362 UK Regulations, above 339, s 22.

detailed approach of the DMCA. As a result, ISPs have to decide whether they accept a notice or not. Under the Directive (but not under the Regulations), anyone can make a notice, whether having legal rights related to the material or not, and not only in writing but also verbally; for example through a phone call, or in any other manner. Unless member states or ISP associations complete the rules, complainants do not need to give their names or addresses. This opens the door to misuses of notice, and puts ISPs in a difficult situation when they have to make a judgement about how well-founded the notice is, and whether there is a chance that it will be followed at all.

Since the Directive does not even mention the notice – only "knowledge", it is left to the ISP to decide whether they "obtained knowledge" by the notice, that is, whether the complaint is well founded, or whether the user has a prima facie defence. This needs expertise and risk-taking, and puts ISPs in a significantly worse situation than the DMCA, which makes it clear that upon notice the material should be removed.[363]

Recital 46 says:

> the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level; this Directive does not affect Member States' possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information.

On the other hand, this may be a benefit to content providers, because their content is not removed automatically – in theory. However, some surveys show that ISPs tend to react without careful consideration of the request.[364]

Recital 40 of the Directive's Preamble encourages that the notice procedure be dealt with in the form of self-regulation:[365]

> this Directive should constitute the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information; such mechanisms could be developed on the basis of voluntary agreements between all parties concerned and should be encouraged by Member States

---

363 Even though at first sight the DMCA version appears to restrict speech more, it in fact restores it by allowing counter-notice.

364 Christian Ahlert, Chris Marsden and Chester Yung, Oxford Centre of Socio-Legal Studies "How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation", July and November 2003 http://pcmlp.socleg.ox.ac.uk/text/liberty.pdf; also see: Nas, Bits of Freedom "The Multatuli Project: ISP Notice & take down" 1 October 2004 http://www.bof.nl/docs/researchpaperSANE.pdf.

365 E-Commerce Directive, above n 71, Recital (40).

Even if ISPs have regulated this procedure in their Codes of Conduct (which the British ISP association has not done), it will be different country by country and may cause differences between the member states, thereby affecting the goal of harmonisation.[366]

An even more substantial difference between the DMCA and the Directive is that the Directive does not provide for replacing the material in case the content provider so requests in a counter notice. This provision of the DMCA tries to put the parties into an equal situation. The Directive places the complainant at a slight advantage: if she claims that an infringement happened, the content is removed at once, and there is no possibility to replace it. In addition, the complainant does not even have to follow a formal procedure to achieve removal of the content. A rational ISP would not comply with a request from a content provider to replace the material, because the ISP would not be protected from liability in that case. For this reason, this question cannot be subject to self-regulation, either. The content provider can not even negotiate or argue with the complainant if she did not leave her name and address behind, which she does not need to under the Directive.

It is true that directives are supposed to give only framework regulation. But it would not be uncommon to set out some requirements that member states would have to meet during their implementation. For example, it could provide that member states are expected to set out the details of a formal notice procedure; and that removed material could be replaced under certain circumstances.

The DMCA provides an even further protection against misuse of complaining rights: it establishes that any person who knowingly misrepresents that a certain material is infringing, is liable for damages arising from that.[367]

As it is seen, neither of these provisions in the DMCA, which try to prevent abusive complaining and balance the situation between the complainant and the provider of the content, are included in the Directive.

A further substantial difference between the two Acts is, that the DMCA has the scope to deal with copyright infringement only, whereas the Directive can be used for all possible illegal content. On the one hand this is beneficial, because it aims at exempting ISPs from the liability for all sorts of content. Simplicity and general coverage are clearly advantages of the Directive. But not all types of illegal content are equally easy to deal with. For a start, unlike copyright infringement, not all illegal content has a certain harmed person. As under the Directive anyone may file a notice: in the case of child pornography or hate speech anybody is allowed to complain. However, in the case of defamation it is much more difficult to tell whether material is illegal than in a copyright or child pornography case. It is easier to tell whether a statement has a defamatory nature, but it can be more

366 Tiberi and Zamboni, above n 340, 51.

367 DMCA, above n 286, (f); see also Tiberi and Zamboni, above n 340, 51.

difficult to decide whether the statement is true or whether the content provider has a statutory defence or privilege to make the statement.[368]

The Directive is at one point narrower than the DMCA: information society service means services that are primarily provided for remuneration.[369] Some authors are concerned about this sentence, because it could be interpreted so that it excludes those service providers who provide free services, among others non-profit universities and libraries.[370] On the other hand, it could also be construed that the definition is to cover services which are usually provided for remuneration. But it does not mean that it would exclude those services of this type, that, exceptionally, are provided for free.

4 Defamation Act 1996 (UK)

The Defamation Act 1996 establishes the defence of "innocent dissemination". It had been designed to provide the defence of innocent dissemination for ISPs. This defence achieves a very similar result to the "mere conduit" rules of the Directive, or even the "safe harbour" of the DMCA. The Defamation Act (the Act) explains in various consecutive levels how this defence can be availed of:[371]

> (1) In defamation proceedings a person has a defence if he shows that--
>
> (a) he was not the author, editor or publisher of the statement complained of,
>
> (b) he took reasonable care in relation to its publication, and
>
> (c) he did not know, and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement.

The sections that follow explain who can fulfil the requirement above in section 1(1)(a). Mainly subsection (e) relates to ISPs but subsections (b-c) could also apply:[372]

> (3) A person shall not be considered the author, editor or publisher of a statement if he is only involved—(...)
>
> (b) in processing, making copies of, distributing, exhibiting or selling a film or sound recording (as defined in Part I of the Copyright, Designs and Patents Act 1988) containing the statement;

---

368 McEvedy, above n 341, 72.

369 The definition of information society services already exists in Community law in Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998.

370 *Bunt v Tilley*, above n 350, 537, Justice Eady.

371 Defamation Act 1996 (UK), s 1.

372 Ibid, s 1(3).

> (c) in processing, making copies of, distributing or selling any electronic medium in or on which the statement is recorded, or in operating or providing any equipment, system or service by means of which the statement is retrieved, copied, distributed or made available in electronic form;
>
> (...)
>
> (e) as the operator of or provider of access to a communications system by means of which the statement is transmitted, or made available, by a person over whom he has no effective control.
>
> In a case not within paragraphs (a) to (e) the court may have regard to those provisions by way of analogy in deciding whether a person is to be considered the author, editor or publisher of a statement.

The last sentence allows a flexible interpretation that may develop with technological development. Subsection (5) gives guidance in the interpretation of s1(1)(b-c):[373]

> (5) In determining for the purposes of this section whether a person took reasonable care, or had reason to believe that what he did caused or contributed to the publication of a defamatory statement, regard shall be had to--
>
> (a) the extent of his responsibility for the content of the statement or the decision to publish it,
>
> (b) the nature or circumstances of the publication, and
>
> (c) the previous conduct or character of the author, editor or publisher.

It is uncertain how the Regulations and the Defamation Act 1996 relate to each other.[374] As Judge Eady pointed out in *Bunt v Tilley*, "there may be circumstances in which the application of the section l defence and of Reg 17 would lead to inconsistent outcomes".[375]

Some commentators are afraid that the United Kingdom could become a target of "libel tourism", because of its plaintiff-friendly laws.[376] Since on the internet everything appears everywhere, even where both the plaintiff and the defendant are foreigners, if the plaintiff claims that she had a reputation in England which has been harmed, they could easily succeed. Several court cases support this suspicion: in *King v Lewis* both the plaintiff and the defendant were Americans, in *Berezovsky v Forbes* the plaintiff was Russian and the defendant American.[377] An

---

373 Ibid, s 1(5).

374 *Bunt v Tilley*, above n 350.

375 Ibid, 543 Eady J, citing Matthew Collins *The Law of Defamation and the Internet* (2 ed, Oxford University Press, Oxford, 2005).

376 Aidan Eardley "Libel Tourism in England: Now the Welcome is Even Warmer" (2006) EntLR 17(1) 35, 35.

377 *Berezovsky v Forbes Inc (No 1)* [2000] EMLR 643 (HL(E)); *King v Lewis* [2004] EWHC 168 (QB).

exception to this trend is shown by *Dow Jones v Jameel*,[378] and *Amoudi v Brisard and JCB Consulting*,[379] where the court found UK jurisdiction was a forum non-conveniens.

5 Copyright

Before the Directive had been passed, the question of ISPs' liability in the field of copyright had been addressed in the Copyright, Designs and Patents Act of 1988. This Act does not expressly exempt intermediaries from liability, but bases liability for copyright infringement upon knowing, or having reason to believe that copyright infringing material is transmitted: "knowing or having reason to believe that infringing copies of the work will be made by means of the reception of the transmission in the United Kingdom or elsewhere."[380]

According to Tiberi and Zamboni it also addresses hyperlinking to infringing material. "If the person who provided the link could be reasonably expected to have been aware that the linked material is infringing, they could be made liable under the secondary liability scheme of section 24(2)."[381]

Also, the CDPA provides that damages cannot be demanded from a person who did not know that an infringement has been committed or had no reason to believe that copyright subsisted in the work to which the action related.[382]

The European Union also issued a Directive regarding copyright matters in 2001, a year later than the E-Commerce Directive. The Copyright Directive[383] limits the liability of those intermediaries who make transient and incidental copies of a copyrighted work in cases where the sole purpose was to enable transmission in a network between third parties, and the acts of reproduction should have no separate economic value on their own.[384] The purpose of these provisions, as declared in Recital 33, is to "enable browsing as well as acts of caching to take place", provided that the intermediary does not modify the information and does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information.[385] The Copyright Directive, however, makes it clear that ISPs should be included

---

378 *Dow Jones v Jameel*, above n 18.

379 *Amoudi v Brisard and JCB Consulting*, above n 19.

380 Copyright, Designs and Patents Act of 1988 (UK), s 24(2) [CDPA].

381 Tiberi and Zamboni, above n 340, 55.

382 CDPA, above n 380, s 97(1); see also Calleja, above n 342, 220.

383 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [Copyright Directive].

384 Ibid, Recital 33 and Article 5.

385 Ibid, Recital 33.

within the obligation to remove infringing material, because they "are best placed to bring such infringing activities to an end".[386]

Therefore, without prejudice to any other sanctions and remedies available, rightholders should have the ability to apply for an injunction against an intermediary who carries a third party's infringement of a protected work or other subject-matter in a network. This ability should be available even where the acts carried out by the intermediary are exempted under Article 5. The conditions and modalities relating to such injunctions should be left to the national law of the Member States.

6 Self-regulation

Self-regulation activities in the UK and the European Union are significant. The first and most wide-known international hotline has been the Internet Watch Foundation (IWF), which is based in the UK.[387] This specialises mainly in reporting and removing child pornography, but it also fights against obscene and racist content, if it is hosted in the UK.

Anyone may report to the IWF online child pornography hosted anywhere on the world, and obscene and racial content if it is hosted in the UK. The IWF investigates the material, and if it is hosted in the UK, requests the ISP remove the material. If the child pornographic material is hosted outside the UK, it reports it to the relevant other hotlines or to the appropriate UK law enforcement agencies. It also recommends ISPs not carry certain newsgroups. It works in partnership with the Internet Hotline Providers Association (INHOPE) and the UK Child Exploitation and Online Protection Centre. The latter passes the relevant information to INTERPOL. The IWF is mainly funded by the internet industry, but it also receives funding from the European Union.

Each year the IWF receives more reports, but every year fewer of the complained sites are hosted within the UK.[388] Whether this is a positive development remains a question, because from the users' (and the childrens') point of view this may not mean a real improvement. The real effect of the fight is unknown. Concentrating on newsgroups is especially futile because after the illegal material is removed from the UK servers, the same material continues to be stored elsewhere.[389]

INHOPE[390] has been founded under the umbrella of the European Union's Safer Internet Action Plan which builds mainly on self-regulation and awareness-raising.[391]

---

386 Ibid, Recital 59.

387 Internet Watch Foundation, established in 1996.

388 Symposium "Governing Pornography and Child Pornography on the Internet: the UK" (2001) 32 UWLA LR 247, 267.

389 Ibid.

390 See INHOPE: www.inhope.org.

Some consider that the undemocratic nature and operation of IWF is a cause for concern, because it exercises quasi-authority functions, while is not accountable to the people.[392] Others say it sets a dangerous precedent for private censorship.[393]

There are several other national and international hotlines. One special focus hotline network is the International Network Against Cyberhate (INACH).[394] This was founded in 2002 by the German self-regulation body Jugendschutz.net in Amsterdam, and is a foundation under Dutch law. It actively searches for racist materials on the net and if it finds it, it requests the ISP remove it. In cases where the material is hosted in a country where it is illegal, it also reports it to the authorities. It had very promising voluntary compliance rates (78%) in the first two years. However, it has not shown much activity in the past couple of years.

E Singapore

The small country of Singapore has achieved a tremendous internet penetration in past years,[395] and is regarded as the high-tech capital of Asia. Because of this accelerated development in the field of information technology, its legal rules have responded relatively rapidly to technological challenges.[396] However, Singapore is not a democratic country and freedom of expression and free press are not an issue for government policy. Therefore its rules cannot serve as positive examples for a democratic country such as New Zealand.

Nevertheless, I found it important to include them in a comparative study such as this one, because the restrictive approach of the Singapore internet content policy reflects the approaches of many other Asian states. Internet penetration in Asia is growing dramatically, and, because of the huge populations of some countries, it presents an enormous market. It is a society with very different values from the western society which – thanks to the internet communication – is emerging from its past isolation. Therefore, in scientific research, it is beneficial to represent it as an example of an alternative approach.

---

391 See SAFERINTERNET: www.europa.eu.int/information_society/activities/sip/index_en.htm and www.saferinternet.org.

392 See Chris Evans "Dictatorship of the Net Censors" (2002) www.netfreedom.org; Sandy Marr "Internet Freedom" (2002) www.newhumanist.org.uk.

393 Geraldine P Rosales "Mainstream Loudoun and the Future of Internet Filtering for America's Public Libraries" (2000) 26 Rutgers Computer & Tech LJ 357, 391.

394 www.inach.net.

395 OpenNet Initiative "Internet Filtering in Singapore in 2004-2005: A Country Study" (2004-2005) 2.B.

396 Amendment of the Broadcasting Act happened in 1996.

1 General overview

Singaporean internet regulation is based upon the Broadcasting Act, and a pseudo-self-regulatory structure; the Internet Code of Practice is issued by the Media Development Authority (MDA),[397] as well as the Internet Industry Guidelines.

The Internet Industry Guidelines declare that MDA takes a light-touch regulatory approach. This may sound somewhat surprising to someone used to the legal systems of old democracies, because the media in general is controlled in minute detail, and heavy sanctions give emphasis to the rules. For example, it is illegal in Singapore to possess radio-communication equipment (a transmitter) and anyone violating the rule is liable to a fine not exceeding SD 100,000, or to imprisonment for a term not exceeding 3 years, or both.[398] The MDA has the right to request any information necessary within any time specified by them:[399]

> The Authority or any person authorised by the Authority in that behalf may by notice require any person to furnish the Authority or the person so authorised, within such period as shall be specified in the notice, with all such documents or information relating to all such matters as may be required by the Authority for the purposes of this Act and as are within the knowledge of that person or in his custody or under his control.

Failure to provide such information results in a fine not exceeding SD 5000 or imprisonment up to 12 months. Any person who commits any "seizeable" offences under the Broadcasting Act may be arrested without warrant and searched by any (authorised) employee of the MDA.[400]

A further example is offered by the MDA Act which describes the MDA's powers as follows:[401]

> The Authority shall have power to do anything for the purpose of discharging its functions and duties under this Act or any other written law, or which is incidental or conducive to the discharge of those functions and duties and, in particular, may

At this point, a list from (a) to (x) follows, where (x) is:

> (x) do anything incidental or necessary to any of its functions, duties or powers under this Act or any other written law.

Beyond internet content regulation, there is a general control of all communication: there are three ISPs in the market, which are directly controlled and partly owned by the government.

---

397 Broadcasting Act 1995 (Sing), s 6.

398 Ibid, Part XI s 47.

399 Ibid, s 50.

400 Ibid, s 52.

401 Media Development Authority of Singapore Act 2002 (Sing), s 12.

The term "light-touch" does not remain without explanation though: it means that licensees will be given a chance to rectify their illegal deeds before the Authority takes action.[402] The MDA has the power to impose sanctions in cases of violation of the code.[403]

The Broadcasting Act differentiates between Internet Access Service Providers and Internet Service Resellers.[404] There are only three Internet Access Service Providers in Singapore, and these are named in the Internet Industry Guidelines: SingNet, Pacific Internet and Starhub Internet.[405] Internet Service Resellers mean schools, public libraries, and cybercafes.[406]

Both types of internet service providers, as well as certain internet content providers (CPs) need a licence to pursue their activity.[407] Internet CPs need a licence only if their web pages are primarily about political or religious issues, for business purposes, or if they are corporate CPs.[408] In other words, CPs do not need a licence if they are private persons, and their content is neither for business purposes, nor about politics or religion, except if notified to do so by the MDA (for reasons that they provide an online newspaper for consideration, or if they provide any programme related to political or religious issues, relating to Singapore).[409]

The licence fee is a discouraging SD 1000 per annum for Internet Access Providers and for those resellers who serve more than 500 user accounts;[410] it is SD 500 for those resellers who serve fewer than 500 user accounts and for localised resellers.[411] Otherwise anyone can apply for a licence, although this seems unlikely.

Internet CPs have to obey the Code of Practice. The Code of Practice says that only those CPs who are licensed need to comply with the code, but the Guidelines do not exempt those who do not need a licence.[412]

---

402 Internet Industry Guidelines, 3f [IIG].

403 Code of Practice s 1(2) [CoP].

404 Broadcasting Act, Chapter 28, s 9.

405 IIG, above n 403.

406 Ibid.

407 Ibid, s 6.

408 Ibid, s 9-13.

409 Broadcasting Act (Sing), Chapter 28, s 9, The Schedule (Para 4) 4-5-6.

410 Ibid, The Schedule (Para4) 2(1)c.

411 Ibid.

412 IIG, above n 402, s 19, but see: CoP above n 403, s 1(2).

ISPs have to remove sites only upon the call of the MDA. They do not need to monitor content, however, they are 'encouraged' by MDA to take their own initiative against offensive content.[413] Further, the Code says "[a] licensee shall use his best efforts to ensure that prohibited material is not broadcast via the internet to users in Singapore."[414]

When subscribing to newsgroups, ISPs are required to make an initial judgement as to the likelihood of a newsgroup carrying illegal material. ISPs are not expected to monitor each posting, they should rather unsubscribe from the newsgroup if it is found to contain prohibited material.[415] For discussion boards or bulletin boards, the website owner is required to exercise editorial rights – and responsibilities. When hosting chat groups, CPs are required to choose discussion topics that are in accordance with the Code of Practice. Although they are not required to monitor the discussion, neither to "censor", they are encouraged to take "discretionary action" against the misusers.[416] Perhaps just to cover any possible loopholes, the Code also says: "in relation to all other programmes on his service, ... the licensee [is obliged to] ensure ... that such programmes do not include material that would be considered to be prohibited".[417]

The list of prohibited materials focuses mainly on sexual materials (including nudity), but also includes advocating homosexuality or lesbianism, and glorifying ethnic, racial or religious hatred, strife or intolerance.[418] Treating politics and religion as sensitive topics is justified by Singapore's multi-ethnic society, and is partly understandable, given the fragile balance between the Muslim, Chinese and Indian parts of the population.

According to research on filtering, there are only an insignificant number of sites filtered in Singapore. Apparently, the intention of the Singapore government is to eliminate only those critical views or that illegal content that originate from within the country, but no real efforts are made to make any foreign content inaccessible. The blocking of a few pornographic sites – among them the most popular but least harmful ones, such as Playboy and Penthouse – appears to be rather symbolic than actually trying to achieve a hermetic isolation such as attempted in China.[419]

The OpenNet Initiative (ONI) found extremely minimal filtering of Internet content in Singapore, as only eight sites of 1,632 tested (0.49%) were blocked: www.cannabis.com,

---

413 IIG, above n 402, s 16.

414 CoP, above n 403, s 2.

415 IIG, above n 402, ss 17-18.

416 Ibid, ss 22-23.

417 CoP above n 403, s 2(3)c.

418 Ibid, s 4(2)(a)(e)(g).

419 OpenNet Initiative "Internet Filtering in Singapore in 2004-2005: A Country Study" (2004-2005) 1.

www.chick.com, www.formatureaudiencesonly.com, www.penthouse.com, www.persiankitty.com, www.playboy.com, www.playgirl.com, and www.sex.com. It is apparent, that this very limited blocking focused on a few pornographic URLs and one site each in the categories of illegal drugs and fanatical religion.

Summarising the findings, it appears that Singaporean regulations cover ISPs and CPs tightly. The regulatory policy targets primarily content providers, trying to prevent by threats of high fines and imprisonment, and wide powers of the police – as in other branches of law – such that no illegal material is published. Although there is no consequent censorship, the wide definitions of "prohibited content", and the obligations of CPs, are tools for the occasionally harsh control, in case it is necessary. Not requiring systematic filtering simplifies the situation for Singaporean law enforcement agencies to a great degree, whereas the general attitude of government and society ensures that transgressions are not significant. Another important element of this regulatory landscape is that Singapore is a small island with a population of 4.4 million, which makes it relatively easy to keep control of the behaviour of the citizenry. The lack of restrictive technological tools and processes also ensure that the technological development and the speed of communication remain flawless.

VII PROPOSAL FOR A REGULATORY SCHEME IN NEW ZEALAND

This part will compare and evaluate the various foreign solutions that deal with ISP liability. It will map the goals to be achieved and the interests that need to be considered. In light of this analysis, it will attempt to propose a few solutions highlighting both their pros and their cons.

A Aspects Taken into Consideration

The goal of this study is to find a solution which settles ISP liability with satisfactory certainty. The sought solution should fulfil the following requirements: providing sufficient certainty for ISPs, not being vulnerable to misuses, observing freedom of expression, efficiently dealing with illegal content, and being cost-effective.

Under certainty, I understood making as it absolutely clear for ISPs what to do in which situation; so that ISPs do not need to make value judgements, let alone legal judgements about the lawfulness of a particular material.

A second aspect of certainty is that the procedure is not vulnerable to misuse. Under misuse I understand it to mean that something is used for a purpose different from its original purpose. This could happen, for example, by targeting the ISP by flooding it with requests, or targeting a content provider – a political opponent or a competitor – to have its lawful content removed.

Freedom of expression is a value that should be preserved, even when occasionally it needs to be balanced with other rights. Stifling speech without such balancing would result a chilling effect which is to be avoided. The internet is a uniquely colourful medium which enables interactive communication for almost every person; it is a realisation of democracy in the original sense of the

word. Trying to suppress speech because it is offensive to some people would compromise this function essentially. Preserving freedom of expression means the protection of the users' interests. Today's procedures focus primarily on the interests of copyright owners and of ISPs; users do not enjoy the presumption of innocence.

Since the procedure is meant to deal with illegal content online, an equally important aspect is how effective a procedure is in doing this. There are various priorities in how to deal with various illegal materials: in some cases, the main purpose could be to remove the content as soon as possible, in others to find the wrongdoer and prosecute, or perhaps demand compensation or rectification. Achieving all these goals at the same time might be too complicated. The solution that is sought is one that is simple and cost-effective. Usually this is coupled with a lack of judicial review, and sometimes also with a lack of ISP-review. Cost-effectiveness and preserving freedom of expression are on the opposite ends of the same spectrum: hopefully a reasonable compromise is to be found.

Below I will evaluate some significant procedures in various countries in light of these values. I select some procedures that are relatively influential and sufficiently sophisticated to be worth the comparison. Some of these procedures are designed to deal with only one kind of illegal content, for example with objectionable content or with copyright infringement. Others have a horizontal effect to cover every kind of illegal content. The procedures have been introduced above in Part III. The following analysis does not discuss the facts again, it only gives an evaluation of the procedures.

B Notice – Classify – Takedown System (Australia)

The Australian Broadcasting Services Act applies a unique solution to deal with objectionable content. The main characteristic of this procedure is that content is removed only upon special order from an authority. This has multiple advantages and only few, but perhaps commanding, disadvantages.

1 Advantages of the procedure

The ISP does not need to contemplate whether material is illegal or not; it is not in a decision-making situation. But removal is not automatic, either. The decision is taken by the ACMA which bases its decision on the judgement of the Classification Board. This ensures that removal happens only if it is well-founded, because the judgement process is carried out by a professional body. For the same reason abusive complaints seem unlikely. Although it is possible to make a complaint anonymously, the complaints arrive at the ACMA, which would filter them.

In order to find offenders, the ACMA may notify the police and request the ISP not to take any action until allowed by the ACMA. Removal of the content is relatively quick, because the ACMA files an interim notice before making a decision, and the deadline is short but reasonably formulated (by 6 pm the next business day). Removal would be quicker only if the ACMA were left out of the procedure entirely, but this would change the whole nature of the procedure.

2 Disadvantages of the procedure

Some of the disadvantages lie in the same facts as the advantages: rating the content and communicating between the authorities is expensive. The material is removed even before the judgement by way of an interim notice. (Although, if the Classification Board does not classify the material as prohibited, it will be replaced.) It remains a question whether some softer forms of objectionable content need such strict attention at all. Censoring simple pornographic content is usually not regarded as a high priority in democratic states. Under the effect of Schedule 5, only the most extreme types of prohibited content are targeted, for example child pornography, but this also may include other extreme content, such as inciting racial hatred:[420]

> (a) describe, depict, express or otherwise deal with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified; or
>
> (b) describe or depict in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not); or
>
> (c) promote, incite or instruct in matters of crime or violence.

No general exemption is granted to ISPs, and there is no other regulation targeting illegal online content and ISPs' relationships to this, except for copyright legislation.

National laws have a narrow territorial effect because they can only target content that is prohibited and potentially prohibited under the national law; and then usually only content that is hosted within the country. Australia aims at being an exception: efforts are made to filter out overseas content and national-server-level blocking comes into policy discussion of the legislature from time to time.

An overwhelming majority of the complaints relate to overseas content (see above). It is hardly worth classifying overseas content, over which Australia has no power. Of course, it is possible to block such content. However, compared to the huge volume of internet content, the few hundred sites that get classified and blocked each year are not significant.[421] It is mainly a symbolic action. Even if they succeed to push out objectionable content from servers within Australia, for the users it does not make a difference whether a site is uploaded in the same country or another.

---

420 National Classification Code 2.1.

421 There were 33 sites found potentially prohibited in November 2006, none of which were Australian; 30 in October, none of which Australian; 34 in September, none of which Australian; 38 in August, from which 1 Australian. See http://www.acma.gov.au.

3 Co-regulative nature

Another special characteristic of this Australian regulation is that it builds to a great extent on self-regulation. So much, in fact, that it is called co-regulation. Elements of state intervention are: (1) the ISP are supposed to make an industry code, otherwise ACMA makes one; (2) the law defines what should be in the industry code; (3) the industry code is compulsory and not complying with it may lead to a fine.[422]

Co-regulation can avail of the advantages of self-regulation without its disadvantages, which arise from self-regulation's voluntary nature; however, it is advisable only in an atmosphere where there is a mutual trust and good relationship between the authority and the industry. In order to avoid centralisation and the impression of direct governmental control, co-regulation should substitute state regulation, rather than self-regulation. Being a soft legal instrument, it is important that its application does not compromise legal certainty.

C Notice-and-Notice System (Canada)

This scheme has been selected because it represents a fresh, new idea among the other notice systems. This is probably the other end of the spectrum than the Australian notice-classify-takedown procedure. Although this had been rooted in self-regulation also, the difference is that this solution interferes to the least extent with content. Of course, there are important differences: first, this is designed for copyright infringements, which are usually regarded as an injury to private interests, whereas the Australian procedure deals with objectionable content which is regarded as injurious to public taste and decency, and potentially harmful to children. Second, this procedure has still not been enacted as a law and it may never be; however, it is used in practice as a form of self-regulation.

In Canada, this self-regulatory initiative is in fact a duty voluntarily undertaken by ISPs. The current copyright law exempts ISPs from liability when acting as intermediaries, without obliging them to take down anything. Although the Copyright Act does not explicitly mention hosting services, this can be deducted from the *SOCAN v CAIP* case where it had to be decided whether caching falls under the exemption.[423]

The task for ISPs is very easy; they do not have to deal with the content at all. Their duty is to send a message to the user, which does not even require that they have a record of the users' identity, because ISPs in most cases would have at least an email address for the user. For the same reason it is cost effective. It is especially favourable to ISPs because it orders that the fee of the procedure be paid by the complainant. The scheme protects the content provider's right to freedom of expression because content is not removed – instead the person has the choice to remove it herself. As long as

---

422 Schedule 5, above n 174, Part 5 Division 4 s 59(1), Division 5 s 68.

423 *SOCAN v CAIP*, above n 228.

the complaint can be filed only with the name and contact address of the complainant, the procedure is not particularly vulnerable to misuses – although flooding an ISP with requests is equally paralysing for the ISP as in the case of notice and takedown procedures. But the content provider is protected against the effects of abusive complaints, because the material is removed only upon her will. Sanctions can be applied only upon a court order.

A further advantage is that it is able to deal with P2P technologies where notice-and- takedown procedures would be useless.

The only disadvantage of this procedure is that it may be relatively slow. The notice goes through the ISP, and a certain reasonable time should be given to the user to terminate the infringing behaviour. If the user does not react positively or does not react at all, the complainant is supposed to sue her (the ISP has to retain identification information about the user for this purpose).

If applied in cases other than copyright, the delay can be regarded as an essential flaw. For defamation or confidential information, such delay may be thought unacceptable. In addition, the content provider's cooperation is less likely in defamation cases, depending on the nature of the content. On the other hand, in alleged defamation cases often the defendant only exercises her lawful right to free speech and judicial review or careful consideration of the material before removal is especially necessary. In such cases the procedure could be completed with a court injunction.

D Section 230 of the Communications Decency Act (United States)

As described above, the interpretation of this rule changed during its lifetime. Both interpretations will be evaluated here.

1 Early interpretation

The unconditional exemption of ISPs from liability – as the CDA was construed between about 1996 and 2001 – was very advantageous for ISPs. The rule was thought to give a clear and plain immunity to ISPs for third party content. The critique was that this made ISPs uninterested in cooperating with harmed persons.

The rule explicitly allows that specific laws depart from it, leaving room especially for criminal and copyright regulation.[424] For example, the DMCA imposed the takedown obligation on ISP in exchange for their immunity.

However, the obligation to remove content and to cooperate with law enforcement in order to reveal the identity of the wrongdoer and immunity are not mutually exclusive concepts. While immunising intermediaries, the law could impose on them the obligation to cooperate under penalty.

---

424 47 USCA, §230, s 230(e) [CDA].

The difference is that the ISPs would not be liable for what someone else did, but for what they failed to do.

Therefore, I argue that the CDA's problem was not that it unconditionally immunised ISPs, but that it did not regulate when and how they should cooperate with infringed parties or law enforcement agencies. In its original form, it did not provide any protection for the infringed person, neither to the public interest. But it protected freedom of expression without any compromises. The preamble of the rule in question gives the impression that this had been the original intention of Congress, namely to protect ISPs and online communication:[425]

> (3) The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.
>
> (4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.

2 Later interpretation

There have been several cases, where an ISP was found immune from liability even though it did not remove material after notice.[426] However, in those cases, which later served mainly as a basis for reconstruction of the rule, ISPs removed material, but refused to give rectification (which is not their obligation in any jurisdiction).[427]

According to the later interpretation, ISPs are not liable as publishers, only as distributors. According to the new interpretation of the CDA, ISPs do not become publishers if they filter or screen content in order to enhance user satisfaction (the Good Samaritan provision). In all other aspects the old common law liability structure remains untouched, the argument holds. For ISPs, this means that after a few years' illusion of "absolute protection", they fall into a state of having no protection whatsoever. The situation in the United States is today very similar to that in New Zealand: there is no specific rule to apply to ISPs' liability, except for copyright issues.

The common law distributor liability means that ISPs are not responsible for content until they have actual knowledge of the illegal nature. They then must take the necessary steps; what the necessary steps are is not defined.

---

425 CDA, above n 424, s 230(a).

426 See *Barrett v Rosenthal*, above n 283; *Doe v GTE Corp* (2003) 347 F 3d 655 (7th Cir); *Austin v Crystaltech Web Hosting* (2005) 125 P 3d 389 (Arizona CA); *Green v Am Online, Inc* (2003) 318 F 3d 465 (3rd Cir); *Schneider v Amazon.com* (2001) 31 P 3d 37; *Gentry v eBay, Inc* (2002) 121 Cal Rptr 2d 703; cited by Machado above n 6.

427 *Zeran No1*, above n 2, *Blumenthal v Drudge*, above n 2.

The lack of protection may have special consequences for access providers. After they are notified about the accessibility of foreign illegal content, they might even be expected to block access to it. Hopefully, this is an unlikely scenario. Blocking content is not expected from ISPs in a democratic country.

The outcome is difficult to predict: striving to avoid liability, ISPs may end up removing all content that they are given notice of, or even block access to it. Malicious notices are able to stifle free expression and get ISPs into trouble.

E Section 512 of the Digital Millennium Copyright Act (United States)

Given its extensive description and its going into minute detail, the DMCA provides relative certainty for ISPs. It describes the procedure to be followed in such detail that there is hardly any flexibility left. This sometimes can cause problems,[428] but its advantage is that ISPs do not have to consider the lawfulness of content. The obvious disadvantage is that all content that is complained of has to be removed, even if the complaint is obviously false. The Act is designed to provide safeguards against abusive notices. For example, the complainant has to give a name, contact address and a statement that they have a good faith belief that the material is infringing copyright. Not everybody is allowed to complain, only someone who is authorised by the copyright holder, which also reduces the risk of malicious complaints.

Still, the Act has some less appealing details. Under close scrutiny, it becomes obvious that it openly favours copyright owners, as is the nature of all notice-and-takedown procedures; the presumption of guilt applies. The attempts to put the user into a better position do not really help an innocent user.

For example, although counter notification is possible, it has a limited scope. First of all, the user can use this option only if she is notified about the original notice. This is not the case under (a), (b) and (d) of the Act (access, cache and searching services).[429] Its scope is further limited by having to make a statement that:[430]

> the subscriber consents to the jurisdiction of Federal District Court for the judicial district in which the address is located, or if the subscriber's address is outside of the United States, for any judicial district in which the service provider may be found, and that the subscriber will accept service of process from the person who provided notification under subsection (c)(1)(C) or an agent of such person.

---

428 *RIAA v Verizon (No 1)*, above n 313.

429 DMCA, above n 286, (g)(2)(A).

430 Ibid, (g)(3)(D).

If the content provider resides overseas, but the content is hosted in the United States, it may be unsuitable for her to submit to United States jurisdiction.[431]

Its effect is also limited, because the counter notice does not immediately result in the replacement of the content. On the contrary, the material can be replaced only after ten days, if the copyright owner does not initiate a lawsuit.

The Act obliges ISPs to reveal the identification information of the user. This helps to find the offender. But, because of a loophole, ISPs must disclose only those clients' identities to whom they provided hosting services, and not those to whom they provided only access services.[432]

When copyright owners request a subpoena to reveal the identity of the user, the user does not receive notice of that. But even if the ISP notifies the user voluntarily, the user does not have the ability to act against the subpoena. Since the *RIAA v Verizon* decision copyright owners start John Doe cases instead of subpoenas against users of access services.[433] The Electronic Frontier Foundation (EFF) criticises the subpoena for being an administrative, rather than a judicial process.[434] Apparently the John Doe lawsuits fulfil the same task, therefore subpoenas seem unnecessary.

Finally, the DMCA cannot respond to the copyright industry's biggest possible concern: P2P applications. Therefore they try to operate with §512(a) repeat infringer rule which may cause real harm to innocent people. Under this rule, copyright holders notify ISPs that a certain user is a repeat infringer (or they send repeated notifications). The ISP is pressed to terminate the account of the user, who does not have any chance to protest against the charge.

The above examples list flaws in the Act which put users in a worse situation than it seems at first sight. Congress tried to design a framework which protects copyright industry and ISPs, but at the same time tried to include some safeguards for users. As we saw, these safeguards are too weak to fulfil their purpose, if their purpose really was to protect the user.

Beyond the problems that are apparent from the text of the law, the practice of the DMCA shows a very high misuse rate. A surprisingly high amount of notices are false, and many are apparently maliciously misrepresenting. Notice is often sent to censor legitimate criticism,[435]

---

431 Electronic Frontier Foundation (EFF) "Briefing Paper: Internet Service Provider Safe Harbors And Expedited Subpoena Process in the US Digital Millenium Copyright Act and Recent Bilateral and Freetrade Agreements" (7 June 2005) 5 [EFF].

432 EFF, above n 431; *RIAA v Verizon (No 1)*, above n 313.

433 Ibid, 8-9.

434 Ibid, 9.

435 Ibid, 4.

commentary and fair use.[436] Although §512(f) provides for sanctioning misrepresentations, the threshold for establishing liability of the complainant is very high: it applies only if a person "knowingly materially misrepresents", whereas for the notice even a "good faith belief" is enough.[437] Apparently, the only case where a court – allegedly even in that case, erroneously[438] – decided in favour of the content provider and obliged the misrepresenting complainant to pay damages, was one which could be won only because the EFF represented the defendants and filed an action under §512(f).[439] In the case *Diebold*, a manufacturer who was often criticised because of the flaws of his electronic voting machines that were to be used in the coming elections, won a court order declaring that emails critical of his products were to be removed from several websites.[440]

Another form of abusive treatment of the process is that copyright owners scan the internet with automated "bots" to find potentially infringing internet content and then file notices without a human review of these hits.[441] Such takedown notices tend to target works that are in the public domain, fair use, book reviews or are simply wrong hits.[442] The complainants' liability cannot be established for such "mistakes" as they are not knowingly made.[443]

Still another improper use of the Act is exploiting the provision (i)(1)(A), which orders that ISPs need to have a policy that provides for the termination of repeat infringers. The DMCA is not suitable to deal with P2P applications where no content is hosted by the ISP. Copyright holders use this section to target those users who are customers only of the access services under §512(a), and where notice or subpoena cannot be applied.[444] Sometimes user accounts are terminated on the basis of a single notice that alleges repeat infringement.[445] Large ISPs are reported to receive tens of thousands such notices a year.[446] Pollack suggests that termination of the user account is not an

---

436 Urban and Quilter, above n 4, 688.

437 DMCA, above n 286, (c)(3)(A)(v); see also Malla Pollack "Rebalancing section 512 to Protect Fair Users From Herds of Mice – Trempling Elephants, or a Little Due Process is Not Such a Dangerous Thing" (2006) 22 Santa Clara Computer & High Tech L J 547, 563.

438 Pollack, above n 437, 566.

439 EFF, above n 431, 4-5.

440 Urban and Quilter, above n 4, 630-631.

441 EFF, above n 431, 5.

442 See also Pollack, above n 437, 560, 563; Urban 673-674.

443 But see Pollack above n 437, 563 "One wonders if automatic searching robot mistakes would be considered "knowing" misrepresentations by copyright holders".

444 See *RIAA v Verizon*, above n 331.

445 EFF, above n 431, 6-7.

446 Urban and Quilter, above n 4, 685.

appropriate sanction (let alone remedy) for alleged copyright infringements, without any court – and particularly, without any human – review.[447]

A further cause for concern is, that notices against search engine links appear to be quite widespread and that a majority of these are false, or even malicious.[448] For example, the Church of Scientology has sent dozens of notices to Google, demanding the removal of links to critical sites.[449] This example is not unique in its nature: many of such notices request competitors' links be removed.[450]

Finally, a malfunction of the seemingly well designed Act is that the (g)(2)(B) counter notification is hardly used in practice.[451] One possible explanation may be that it is easier for the content provider to replace the material themselves, perhaps through another ISP.[452] A second reason may be that the possibility of counter notification is simply not known. A further problem is that when termination of account occurs due to a notice, the customer does not even need to receive a copy of that notice, and does not have the chance to file a counter notice at all.

F Electronic Commerce Regulations (UK)

This scheme follows the typical distributor liability structure. It has its roots in the Electronic Commerce Directive of the European Union,[453] and is only a little more detailed. It is also very similar to the DMCA, especially in its definitions.[454] However, it lacks a number of elements of DMCA. The lack of these details may result a lessened security on the one hand, but possibly fewer opportunities for misuse on the other. Unfortunately, no factual research regarding this procedure has been undertaken comparable to that undertaken concerning the DMCA practice. One reason may be that this was enacted more recently, six years after the DMCA.

A typical characteristic of this scheme is that ISPs have to decide whether material is unlawful or not. A notice can be a sign that the ISP had knowledge of the illegal material, but it does not necessarily help the ISP decide whether the claimed material was really illegal. This may impose a burden on ISPs who have to check whether the notice is legitimate. On the other hand, it is better for

---

447 Pollack, above n 437, 574-575.

448 See Urban and Quilter, above n 436.

449 EFF, above n 431, 5.

450 Ibid; Urban and Quilter, above n 4, 654-655.

451 Urban and Quilter, above n 4, 679-680.

452 Ibid, 680.

453 E-Commerce Directive, above n 71.

454 See for example DMCA above n 286, (a-b); UK Regulations, above 339, 17-18.

users because their content is not removed automatically. ISPs are not relieved from the liability towards their users, whose potentially lawful content they have removed.

The scope of those persons who can make complaints is wider. Although they have to give their full name and address, they do not need to be authorised by the harmed person. This is understandable, given that the Regulations extend to all sorts of illegal content, such as racially discriminative speech, which do not have one specific victim. However, this could make the procedure susceptible to misuses.

The interests of the harmed person (or the public) are well protected, because ISPs are interested to remove the content as soon as possible, to avoid liability. (It is not defined what time-span is available for ISPs to do this – but this will likely develop in practice.)

The Regulations do not require that ISPs keep data on the infringing users or reveal them to a private person upon request or subpoena. But other laws may achieve the same purpose. The Data Protection Act 1998 of the UK requires keeping personal data confidential generally, and allows exceptions where data is necessary for the purpose of legal proceedings or otherwise necessary for exercising legal rights.[455] However, there is no obligation to disclose, only a possibility.

The Regulations do not acknowledge "counter notice", that is, the request of the content provider to put her content back. In absence of such legal authorisation, ISPs would not risk putting back content that has been removed once, because that could establish their liability. Not only is content removed without any prior judicial review, but there is no chance to have it put back – this is clearly a burden on freedom of expression. If the content provider wants to have her content replaced, she has to sue the complainant – provided that he or she left a name. Or, she should sue the ISP – which constitutes the failure of the whole procedure, which was originally meant to relieve ISPs from liability. Considering that a malicious and anonymous complaint may cause the removal of lawful material, and the CP has no right to remedy whatsoever, this procedure seems to put a heavy burden on freedom of expression.

G Comparisons

In the table below I indicate those aspects that I examined, with values from 1-3, where one means that the value is not fulfilled, 2 means that it is not always, or not fully achieved, and 3 means that it is fulfilled.

---

455 Data Protection Act 1998 (UK), s 35.

Qualities of the procedures	ISPs' legal certainty	Not vulnerable to misuses	Quick removal	Finding offender	Freedom of expression	Cost-effective	*Sum*
Notice-Classify-Takedown (Australia)	3	3	2	1	3	1	*2.17*
Notice-Notice (Canada)	3	3	2	2	3	3	*2.67*
CDA orig.interpr.	3	3	1	1	3	3	*2.33*
US CDA distributors	2	-	3	1	1	3	*2.00*
US DMCA	3	2	3	3	2	3	*2.67*
UKRegulations	2	1	3	1	1	3	*1.83*

Figure 1[456]

The table shows what has been explained above. All procedures provide a certain level of legal certainty for ISPs, but the distributors' liability structure provides less, because ISPs have to decide themselves whether content is illegal or not. In fact, the distributors' structures add very little to the general legal rules: they merely set the threshold of liability at intentional wrongdoing.[457] ISPs are not protected against users' anger after removal: they have to take the risk of being overly cautious, as well as being less cautious than is necessary.

Only those procedures where content is not removed, or where it is removed only after a formal review, are not vulnerable to misuse. Although the DMCA provides safeguards, in practice they seem not to fulfil their role. In absence of such safeguards, the notice-and-takedown scheme of the UK Regulations is even more exposed to misuses. The later interpretation of the CDA (the distributors' liability regime) does not give instructions as to what exactly ISPs should do if they encounter illegal content – therefore this aspect could not be evaluated.

---

456 Please note that the figures may be distorted depending on which procedures and which values are included. The average should not be regarded as an objective average value; it depends on the situations examined which may not be regarded as representative.

457 ISPs can not be made liable for negligent action, because actual knowledge is required to establish liability.

The speed at which the removal of the illegal content can be achieved may be an important aspect when the original situation cannot be restored, such as in the case of confidential information. Here the leading procedures are those which perform less eminently in the other aspects, namely, the notice-and-takedown schemes. Of course, the quick and often automatic removal is the cause of all the other problems, which will mainly culminate in the unnecessary restriction of freedom of expression.

Finding the offender is not really a function on which most procedures concentrate. In fact, it is only the focus of the DMCA, which provides for preserving and revealing user data upon request. However, even this Act did not cover the situation of P2P applications, therefore copyright owners are confined to use the general method, and file John Doe suits against the anonymous users. As is seen in this example also, other, probably already existing, legal rules can deal with this problem satisfactorily. Therefore I leave this aspect outside the scrutiny below.

Freedom of expression is preserved in those procedures which do not remove content without the users' consent, or without a formal review. This value produced the lowest marks in the distributors' liability structure and the "simple" notice-and-takedown systems, because in those, ISPs are motivated to remove all suspicious content. They can arrange to exclude liability towards their clients in the user agreements. The DMCA received a medium mark, because it provides for replacing the content upon the users' request. Unfortunately, as discussed above, this possibility is not exploited by the users.

Finally, all procedures are relatively cost-effective, except for the one where authority review is included. Misuse of procedure can raise the costs significantly, as shown by research where ISPs receive tens of thousands of false notices a year.[458] Therefore, cost-effectiveness should be interpreted in a wider context. First, how much does it cost for the ISP, but also how much does it cost to users (for example when their account is terminated), and how often are subsequent lawsuits necessary to clarify the situation?

458 Urban and Quilter, above n 4.

The same data is shown below in a visual layout.

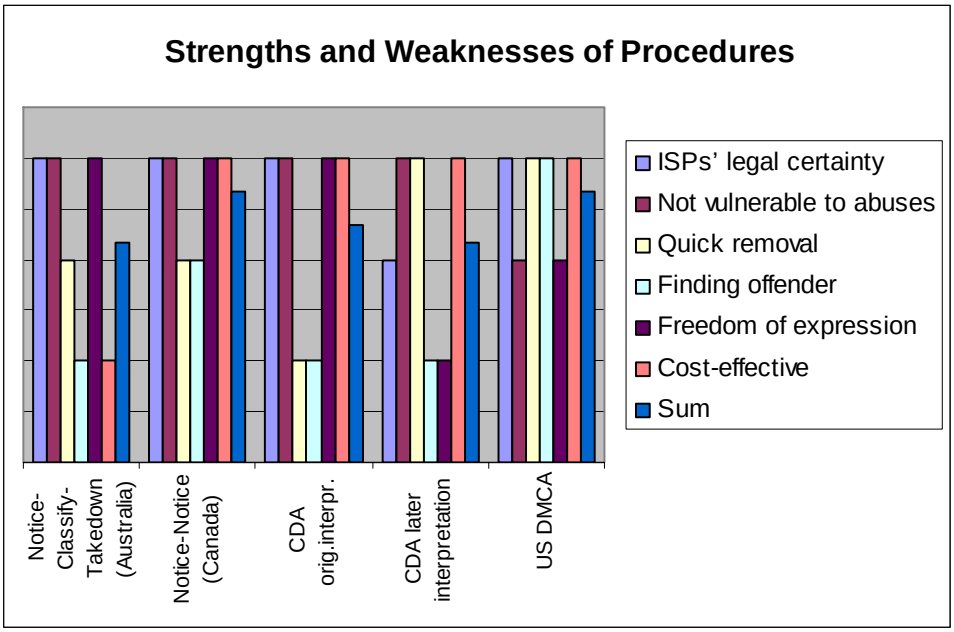

Figure 2

As we know, the values listed here do not enjoy the same importance in every case. There can be cases where finding the perpetrator is a high priority, whereas in others nothing more than a quick and easy removal is necessary. The next table represents some of the most typical illegal content that causes concern on the internet, and the priority goals that can be attached to the different types.

Priorities	**Child pornography**	**Copyright**	**Defamation**	**Privacy**	**Hate speech**	***Average***
Quick removal	3	1	3	3	2	*2.40*
Finding the wrongdoer	3	1	2	1	2	*1.80*
Invulnerable	1	3	3	3	2	*2.40*
Freedom of Expr	1	2	3	2	3	*2.20*
Cost Effectiveness	2	3	2	2	2	*2.20*

Figure 3

I left out from this table "ISPs' legal certainty" and "the procedure's invulnerability to misuses", because they are regarded as generally important in all types of cases.

Quick removal is less important in copyright, because the damage caused in terms of the loss of income by copyright owners is not influenced by a few days.[459] Its importance is medium in case of hate speech, only because it may contain threats. The real important cases where removal has to be quick are defamation and privacy (as well as confidential information), where the harm is virtually not restorable, and child pornography, where the interest of an actual child are compelling.

Finding the wrongdoer has special importance in child pornography, and publication can lead to finding the perpetrator who committed the more serious crime: taking the photographs. Finding the wrongdoer may still be important in cases of defamation and hate speech, for the purposes of demanding rectification or compensation (and, where criminal liability is attached to one or to the both, for prosecution). But, in copyright infringement, because of the volume of a "pirate", who has relatively little effect on her own, it does not have much importance. In privacy finding the publisher is not a priority, although compensation may be demanded, but the damage to the privacy can not be restored.

I measured the importance of the procedure's invulnerability by the likeliness of misuse. For example, child pornography is not likely to be falsely notified, or at least not maliciously, whereas in the case of defamation or privacy a maliciously false notice is more probable. However, as it was shown above, even procedures designed against copyright infringement can be misused to get rid of competitors. In other words, even a procedure which is the most minutely regulated and equipped with safeguards can be misused.

Freedom of expression is detailed according to its relevance as well: there are cases where it is more likely to be relevant. For example, in relation to child pornography we usually can not talk about a right to freedom of expression, whereas in the case of defamation, it always has to be balanced with the plaintiff's right to reputation.

Cost effectiveness is reasonably important in all cases; it is a special priority in copyright cases, because the whole purpose of copyright protection is commercial and only rarely moral. The other cases allow more flexibility regarding the costs, because the procedure has a public importance.

How well freedom of expression is respected by a procedure can be measured by various characteristics: first of all, whether the content is removed without the users' consent or a judicial review. A further factor is how easy it is for the complainant to achieve removal, and whether the

---

459 Some studies argue that it is a myth that music industry suffers a loss because of file-sharing. See Pollack, above n 437, 549; Michael Geist "Piercing the Peer-to-peer Myths: An Examination of the Canadian Experience (2005) First Monday.

user has a chance to act against it. Does the complainant have to leave her name and address? Can the user get her content put back?

Legal certainty and freedom of expression are also correlated. If ISPs are not certain about the limits of their liability, or if they have to decide what is illegal and what is not, they are likely to "shoot at everything that moves" and remove more content than strictly necessary. This overreaction has happened even in the case of child pornography, for example where a picture of a little girl with a lollipop was regarded as pornographic.[460]

The same data on a visual layout in Figure 4:

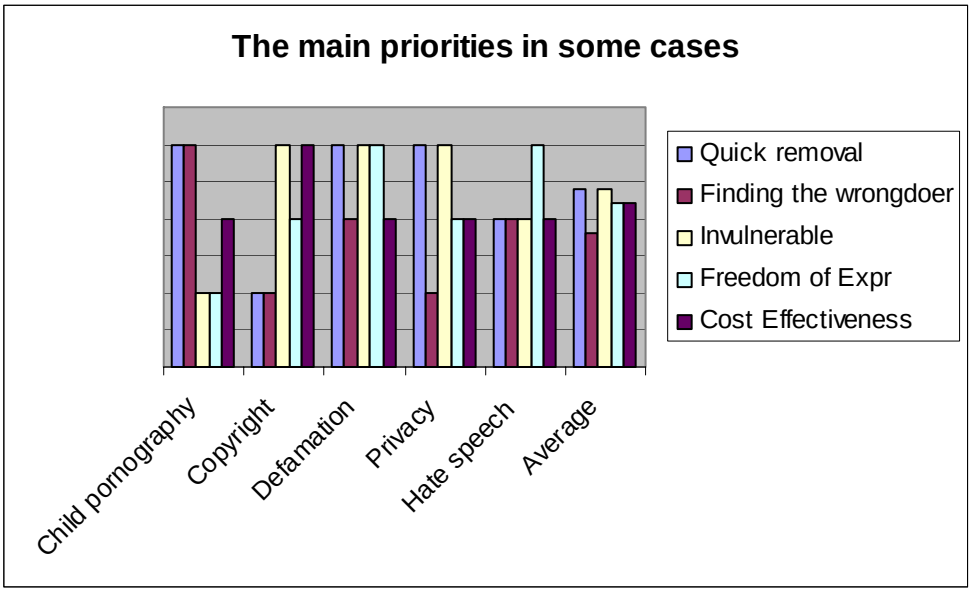

Figure 4

Depending on which goals are most desired, it is possible to compare the procedures with each other. For example, if we are interested in quick removal, all the notice-and-takedown systems perform well. However, if we are more interested in preserving freedom of expression, or designing a system that is not vulnerable to misuses, then notice-and-notice, notice with a judicial review, or absolute immunity might serve better.

---

460 See also Philip Jenkins *Moral Panic: Changing Concepts of the Child Molester in Modern America* (Yale University Press, New Haven,1998)

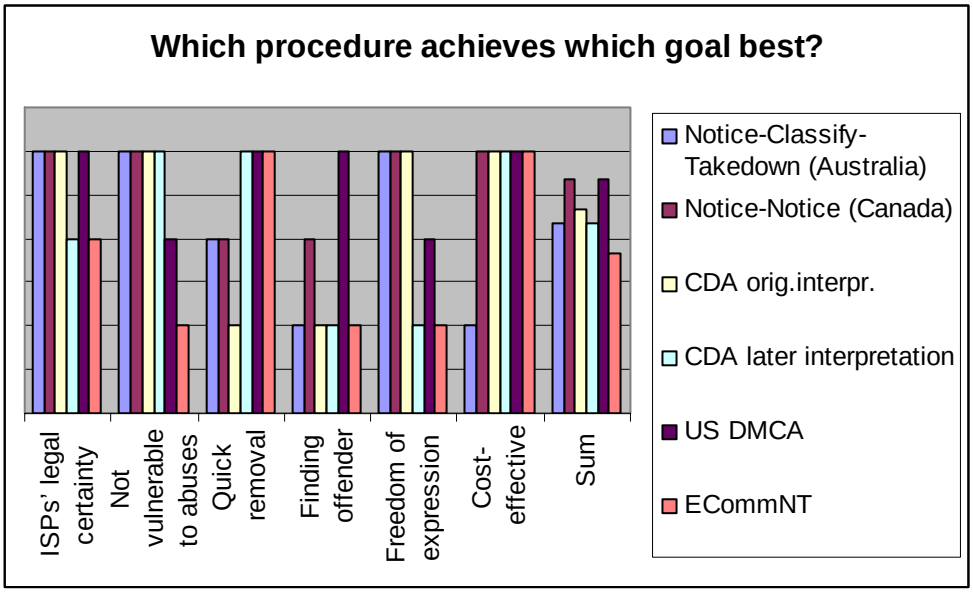

Figure 5

The goals cannot be achieved all at the same time, because some of them mutually exclude each other. A procedure that includes judicial review cannot be among the cheapest ones. One which respects the rights of the harmed person to a great extent (which is acceptable in the case of child pornography) is bound to restrict freedom of expression.

Note, that the numbers are purely symbolic, and they do not express any quantitative measure. The row of aspects can be extended or narrowed, thus changing the "average" result. However, as a result of this analysis, it is indicative that the highest values can be attributed to the notice and notice system which is the newest phenomenon and developed by the industry itself, and the DMCA which is the pioneer among notice-and-takedown systems, and the most sophisticated of its kind. However, the research into the practical application of DMCA is disappointing.[461] Studying the chart carefully, it is conspicuous that the DMCA does not perform well in average, but it has one value which is outstanding; finding the perpetrator. However, as above,[462] although the text of the Act provides for disclosing user data, this cannot be applied under the circumstances of P2P applications, which make up the bulk of piracy, and the copyright holders use John Doe procedures instead. Given, that this aspect was found to be the least important on Figure 4, (in fact it only had a

461 See Urban and Quilter, above n 4; Pollack, above n 437.

462 See DCMA, above n 286.

priority in case of child pornography) and considering that the same goal can be achieved with other means, I will eliminate this aspect in the following chart (Figure 6):

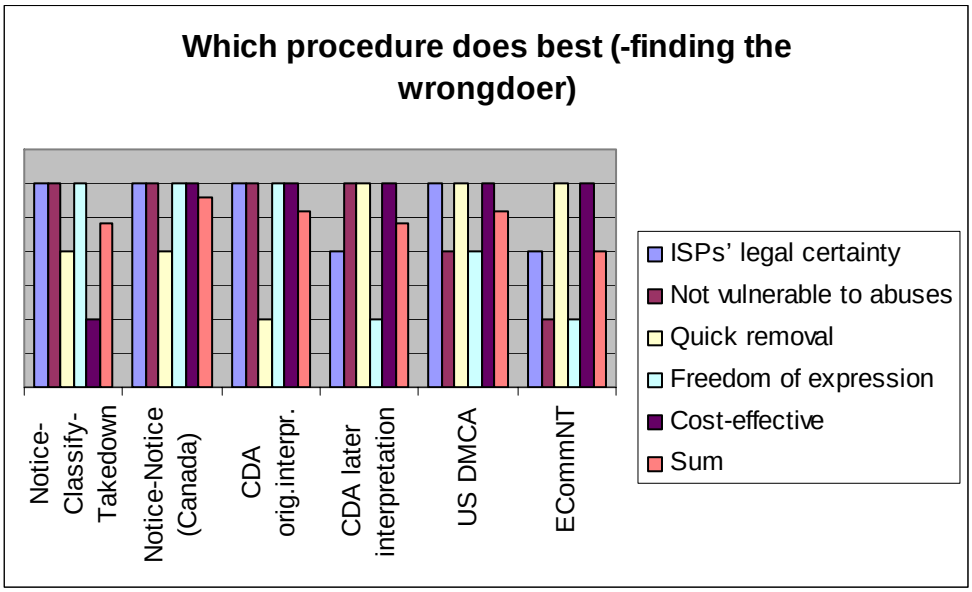

Figure 6

Looking at the "Sum" columns, it is conspicuous that now it is the notice-and-notice procedure which has the highest average, and the DMCA is not better than the original interpretation of the CDA (for difference reasons; that interpretation was thought to provide unconditional immunity to ISPs).

Notice-and-notice procedure stands out in four categories: it provides legal certainty for ISPs, it is not vulnerable to misuses, it preserves freedom of expression, and it is cost-effective. Its only drawback is that it is less likely to result in a quick removal. Therefore, for those cases where it is highly important to remove the material quickly, like in child pornography and privacy, as shown in Figure 4, this is not the best solution. But in copyright and hate speech issues notice-and-notice may be the best.

H Alternatives

As stated above, a general solution should achieve the following goals: legal certainty for ISPs, invulnerability of the procedure, quick removal, maintenance of freedom of expression, and cost-effectiveness. Apparently, there is no procedure that would achieve all goals. There are more alternatives in this case:

(a) While realising the main goals, the hindrances are minimised by complementary measurements.

(b) Different procedures are selected or designed for the different problems, and incorporated in the various different laws.

1 Advantages that mutually exclude each other

Based on the above analyses, the following can be concluded:

(I) A procedure can:

- provide ISPs with full certainty;
- be less vulnerable; and
- respect freedom of expression,

but

- not remove material quickly; or
- not remove material at all, and then it is cheap but not effective; or
- it will provide for removal of material upon a judicial review, in which case it will be expensive; or
- remove material with the consent of the content provider, and in some cases upon a judicial order.

(II) A procedure can quickly remove material, but thereby be vulnerable to any misuse, and

- either provide the ISP with certainty but then seriously restrict freedom of expression (because of automatic removal),
- or put ISPs in a decision-making situation and still restrict freedom of expression.

In the first sub-point, the content provider bears the burden of misuse, in the second, the ISP does, who has to review all complaints.

2 Risk and cost management

The risk and the costs somehow should be divided between the content provider, the ISP and the harmed persons. The following schematised chart shows how the risks are divided today in the known foreign procedures.

Risk-and-cost division	Harmed person	ISP	Content Provider
Notice-Classify-Takedown	2	1	1
Notice-and-notice	1	1	1
CDA original	2	1	1
CDA distributors	1	2	3
DMCA	1	1	3
UK Reg	1	2	3

Figure 7

In the case of the Australian notice-classify-takedown procedure I took the public as a harmed person, first because there is no specific damaged person, and second because it is the public authority which initiates the procedure. Here the risks of the ISP and of the content provider (CP) are not significant because the ISP is not in a decision making situation, and the CP's content is removed only if it is legitimately done so.

In the notice-and-notice procedure, none of the parties risk too much: the harmed person risks only that the harmful content is removed a few days later, or that she has to sue the CP in order to have it removed. I refuse to interpret this as a "risk", because it is nothing more than what any person should expect when publication is made in another media. In addition, the planned notice-and-notice procedure provides for revealing the user data upon request which makes suing easier for the harmed person.

In the CDA's original interpretation the harmed person can also have the content removed only upon a court order, but has to request the user data in a specific court (John Doe) procedure.

In the distributors' liability structure (which is in fact a common law liability, left untouched by the CDA, and the same in the UK Regulations), the harmed person has a good chance that the content he has complained of will be removed by the ISP. The ISP, however, is in a decision-making situation: is the content in question illegal or not? The user faces a risk that her content will get removed without a real, legitimate ground. This risk is still lower than the risk a user faces under the DMCA: where all notice must result in a removal. In the case of DMCA, the ISP does not have to decide: it is in a clear position. The complainant has no risk, either, because she can easily achieve removal of the objectionable content. All the risk and burden is carried by the user.

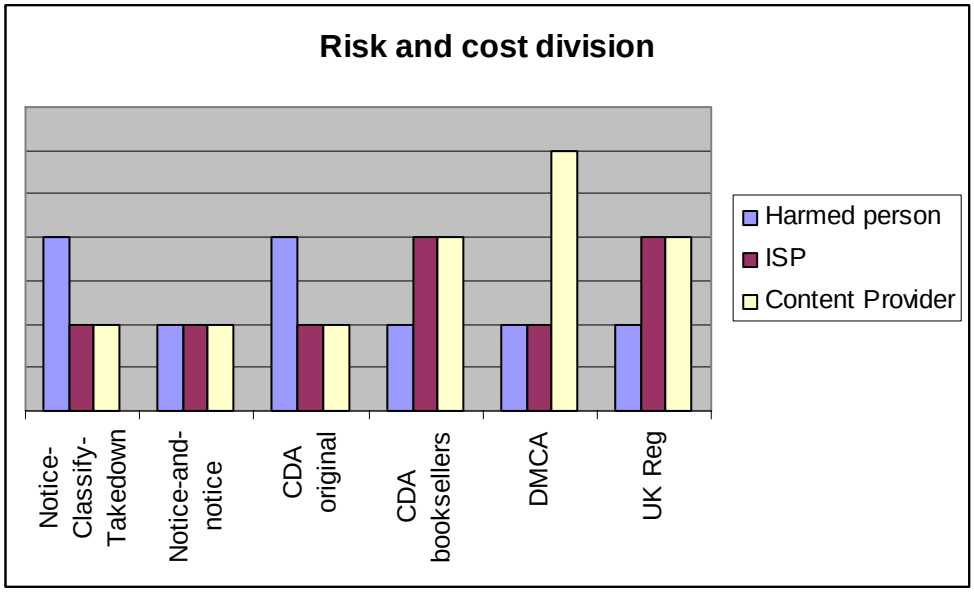

Figure 8

It stands out that in the DMCA procedure the user (and her freedom of expression) bears most of the burden. This is mainly because both copyright industries and telecommunications industries managed to realise their interests.[463]

This burden has proved to be high in fact because of the thousands of false notices which go through ISPs unchecked. In the bookseller liability structures (CDA and UK Regulations) the risk for users is smaller only because the notices are filtered through the ISPs, who have to make a decision about the lawfulness of the material. Therefore, in fact the risk is shared between users and ISPs.

My question is: is it fair that any person can make a complaint about any matter, and the ISP has to go through the notices and select, like Cinderella, which one is well-founded and which one is not?[464] Adding to this, the fact that ISPs act under the threat of being charged for the content if they make a mistake? (This is in contrast to the administrative liability for cooperating as described in the notice-and-notice procedure.) If ISPs are expected to act "expediently" upon the notice, it is a minimum expectation that the notice is expedient itself.

---

463 See Pollack, above n 437, 555-559.

464 As it is under the CDA and the UK regulations.

Although we do not have data about misuse of the procedures in other countries, we do not have any reason to think that the procedure will not be misused elsewhere than the United States. The burden on checking which notices are legitimate and which are not,should not be carried by ISPs, and it should not be carried by the user either. The DMCA sanctions wilful misrepresentation, but the threshold for establishing it is so high that practically it cannot be applied. In addition, no procedure should force a person who exercised a free speech right to initiate a lawsuit to be able to continue to exercise this right.

VIII THE PROPOSAL

As a result of these analyses, my proposal is to take the notice-and-notice procedure as a basis, with some additions for special situations. These additions are:

(1) Immediate removal upon judicial order.

(2) A separate procedure for child pornography, to be detailed below.

(3) A general declaration to exclude liability of access providers, hosting providers, those hosting cache copies and search engines for third party content. Definitions on access, cache, hosting and searching services could be similar to the DMCA or the UK Regulations.

(4) ISPs must retain user data; but disclose it only upon judicial order, unless as described in point 9 below.

(5) If the user is truly anonymous (the ISP does not have any contact information), the content shall be simply removed. The user shall have the possibility to request that the content is replaced, by giving her name and address. The complainant shall be notified of this and given the name and address of the user.

(6) Search links and cache copies should be removed if the ISP learns that the original content has been removed.

(7) User accounts may be terminated only upon a court order or the ISP's own decision. It should be used sparingly because terminating or suspending an account deprives a user of basic information needs, possibly a work tool, and punishes other people who live in the same household.[465]

(8) The user must be informed in the notice that if content is not removed within a defined time, her data will be forwarded to the complainant who may sue her.

(9) User data shall be given to the complainant if the user does not remove the content within a reasonable time (for example, eight days). Before this time, it can be revealed only upon a

---

465 See also Pollack, above n 437, 573.

court order. The ISP should retain the user data from the time of the notice. Complainants' data shall not be given out to users unless the complainant requires so.

(10) If the user data is or turns out to be pseudo-data (for example, a nickname, or an anonymous email address), and the user does not remove the content voluntarily, the complainant shall have the ability to request a court injunction against the specified content and the user as specified by its username.

(11) ISPs shall be obliged to follow this procedure under threat of a fine.

1 Characterisation of this procedure

(a) ISP point of view

The ISP does not have to judge whether the complaint is legitimate or not. All it has to do is to cooperate with the complainant and the user. If it finds that the user cannot be contacted, for example, the email address given does not exist, it should remove the content. However, even in this case the ISP is obliged to make a reasonable effort to establish contact with the user, for example, to check if the email address was not misspelled and if the user's address is not known from a public register, from the website, or otherwise available. The ISP does not have to make legal judgements about the lawfulness of any content. It has to maintain fair communication towards both parties and notify both parties about all moves it makes during the procedures.

(b) Harmed person's or public point of view

The harmed person can choose the easy solution, which is to notify the ISP and wait for the user to remove content; or the secure solution, which is to ask for a court injunction to terminate user's illegal activity immediately. To do this, it can get the user data from the ISP or have the ability to request a court injunction against certain content and the user specified by username.[466] If the harmed person wants to demand damages from the user, she can do so. As Ehrlich argued, "[t]he real obstacle for victims is not the absence of distributor liability for ISPs[,]… [but] the cloak of anonymity available to bad actors."[467]

If the user is truly anonymous, the content is simply removed. The procedure can deal with file-sharing and other P2P applications.

(c) Point of view of the user

---

466 It should be possible to get a court injunction without knowing the identity of the user. For example, that the comment number 64117 of Bloody666 from the forum "chicks&boys" from www.teensanger.com website be removed.

467 Ehrlich, above n 269, 418.

The content is not removed without the consent of the user, unless she chose to be truly anonymous, or unless a court orders so.[468]

(d) General evaluation:

The procedure is not likely to be misused. Still, the following misuses can be imagined: (a) court injunctions and identity disclosure orders are issued very easily and some persons use them to stifle criticism or competitors; (b) ISPs receive so many notices that it is a significant cost to deal with them: (c) users do not remove their content but move to another ISP every time. Unfortunately, it is impossible to exclude misuses entirely. These risks are apparently not different, but perhaps less likely than the dangers of other procedures.

The procedure does not require costly investments from any of the parties. It may seem that the harmed person is in a worse situation than under the DMCA – this is indeed so, because under the DMCA sending a notice was enough to get any content removed. There has been no other time in history when a person had such a power over other persons' speech. There is no reason why this should be so in the internet era.

The internet has sped up communication – so why not exploit this speed in conflict resolution as here? And this is only a first step towards a completely online mediation procedure.

Finally, this is the only procedure at hand today which is able to deal with the newest and most widespread communication technology: peer-to-peer content. Since this is the biggest concern for both copyright owners and police, it is absolutely necessary to target this problem.

2 Dealing with child pornography

For dealing with child pornography, I propose a modified distributors' liability scheme for hosting providers, and a modified notice-and-notice scheme for access providers. Note that these alternatives are proposed solely for child pornography which is a crime, and not for objectionable content in general.

(a) Hosted content

If the ISP is notified about hosted child pornographic content by a hotline or the police, or otherwise has actual knowledge about the content, it has to remove that content under the penalty of a fine, and notify the user. The ISPs should abstain from removing material if the police so request.

(b) Explanation

My proposal is that the ISP has to remove material upon actual knowledge, and if notice is received from a hotline or the police. No automatic reaction upon notice from the general public shall be required. The reason to place more liability on ISPs in this aspect is that distinguishing child

---

468 But see Pollack, above n 437, 574-575.

pornography is relatively easy (even when there are occasionally ambiguous cases). Nevertheless, ISPs should not face charges of distributing child pornography even if they fail to remove illegal content. Therefore, they should be threatened by a fine instead, while their immunity is declared in general.

(c) File sharing

If an ISP becomes aware of child pornography being distributed through a P2P system, it should notify the user. In case of repeated infringements it may be required to inform the police.

It is a question of policy whether ISPs should inform the police at the same time as the user. There is currently no obligation to denounce distribution of child pornography. Through file sharing applications many innocent users may inadvertently download disguised child-pornographic images. Users often do not open the files that they have downloaded, because they do not have enough time to.[469] Therefore raids into users' computers shall be done with respect to the presumption of innocence. My proposal is that if the police have a prior suspicion about someone, they should be able to ask an ISP not to inform the user. But I cannot recommend that ISPs denounce potentially innocent users with such a stigmatising crime without notifying the users at the same time.

3 Second layer service providers

For so-called second layer ISPs, like blogger-sites, universities, as well as social network sites, such as MySpace and YouTube, which are growing in number and popularity, I propose a traditional distributor-type liability. These sites are not ISPs in the original meaning of the word, because they do not provide network services. They provide content templates and enable user communications. They specialise in dealing with content, and invite certain types of content to be hosted by them. They usually provide their services free to users, and do not require authentication. These are the reasons why they should be treated differently from ISPs. They can be regarded as distributors in the original sense of the word: like a traditional library which collects books. They should not be liable until they have actual notice about the illegality of certain material. After they have actual knowledge of it, it should be their responsibility to remove it or otherwise deal with it.

Unlike ISPs, they should be liable for not removing the content as if they provided the content themselves. The reasons are:

- They specialize in inviting certain types of content, for example ,YouTube.
- They often do not hold identity details of their users and if they do, they would often be unwilling to disclose them.

---

469 In today's attention economy, it is not uncommon to collect vast amounts of information with a mouse-click or two, and never come to actually view it. See also Davenport and Beck *The Attention Economy: Understanding the New Currency of Business* (Harvard Business School Press, Boston, 2001).

- Usually they work with smaller amount of data than ISPs.[470]
- They are not indispensable mediators of internet communication. Users can find other ways of expression if their content is removed or even if they are banned from the site. If users wants to express their ideas independently and without control, they can have their own websites.

I regard these places as social places, whereas ISPs provide the "home" for users, the most basic facilities such as internet access and an own homepage. In contrast, second layer ISPs are functional gatherings for certain activities, where users may be expected to respect the social rules and accommodate others.

470 Although this mainly depends on the market position of the particular ISP and the particular second layer service provider.