***CATCHWORDS – FREEDOM OF INFORMATION –*** *Whether Universal Resource Locaters and Internet Protocols of Internet content that is prohibited content or potentially prohibited content are exempt – whether disclosure would, or could reasonably be expected to, have an international adverse effect on the proper and efficient conduct of the ABA's operations – decision affirmed.*

*Freedom of Information Act 1982 ss. 3, 4, 11, 12, 13, 24, 24A, 37, 40, 41, 43 and 112*
*Broadcasting Services Act 1992 ss. 3, 4, 5, 40, 158, 159 and 216B, Schedule 5, Clauses 1,2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14 to 21, 24, 24A, 27, 30, 40, 58, 59, 60, 62, 63, 66, 68, 69, 70, 71, 76, 79, 82, 83, 85, 92, 94 and 95*
*Broadcasting Services Amendment (Online Services) Act 1999*
*Crimes Act 1914 s. 85ZE*
*Classification (Publications Films and Computer Games) Act 1995 ss. 12 and 27*
*Censorship Act 1996 (WA) ss. 81, 99, 101, 102 and 105*
*Classification (Publications, Films and Computer Games) (Enforcement) Act 1995 (ACT) s. 24*
*Classification (Publication, Films and Computer Games) Enforcement Act 1995 (Tas) ss. 71, 72 and 74*
*Classification of Publications, Films and Computer Games Act (NT) ss. 50Z, 50ZA and 50X*
*Classification (Publication, Films and Computer Games) (Enforcement) Act 1995 (Vic) ss. 56, 58 and 59*

*Attorney-General's Department v Cockcroft (1986) 64 ALR 97*
*Re Bayliss and Department of Health and Family Services (AAT 12277, 10 October, 1997)*
*Re Connolly and Department of Finance (1994) 34 ALD 655*
*Re James and Australian National University (1984) 2 AAR 327*
*Searle Australia Pty Ltd v Public Interest Advocacy Centre and Another (1992) 16 AAR 28*
*Re Booker and Department of Social Security (AAT 6189, 13 September 1990)*

## DECISION AND REASONS FOR DECISION

**ADMINISTRATIVE APPEALS TRIBUNAL )**
**) Q2000/979**
**GENERAL ADMINISTRATIVE DIVISION )**

**Re ELECTRONIC FRONTIERS AUSTRALIA INC.**

**Applicant**

**And AUSTRALIAN BROADCASTING AUTHORITY**

**Respondent**

## DECISION

| | |
|---|---|
| **Tribunal:** | Miss S A Forgie (Deputy President)<br>Mr I R Way (Member) |
| **Date:** | 12 June, 2002 |
| **Place:** | Brisbane |
| **Decision:** | The Tribunal affirms the decision of the respondent dated 6 September, 2000 affirming its earlier decision dated 21 July, 2000 |

**S A FORGIE**
**Deputy President**

## REASONS FOR DECISION

On 18 October, 2000, the applicant, Electronic Frontiers Australia Inc ("Electronic Frontiers"), applied for review of a decision of the respondent, the Australian Broadcasting Authority ("ABA") dated 6 September, 2000 affirming a decision dated 21 July, 2000 to refuse access to certain documents under the *Freedom of Information Act 1982* ("FOI Act").

2. Electronic Frontiers' Executive Officer, Ms Graham, represented it at the hearing and Ms Campbell represented the ABA. The documents lodged pursuant **s. 37** of the *Administrative Appeals Tribunal Act 1975* ("T documents") were admitted in evidence together with affidavits of Ms Andree Margaret Wright (the Director of Policy and Content Regulation at the ABA) and of Mr Richard James Fraser (the acting Manager of the Online Services Content Regulation Section of the ABA) and the *Guidelines for the Classification of Films and Videotapes* (Amendment No. 3) approved under the *Classification (Publications Films and Computer Games) Act 1995* ("Classification Act") ("the Guidelines"). Oral evidence was given by Ms Andree Margaret Wright and Mr Richard James Fraser.

### THE ISSUES

3. The issues in this case are whether documents are exempt pursuant to either **ss. 37(2)(b)** or **40(1)(d)** of the FOI Act in so far as they reveal Universal Resource Locaters ("URLs") and Internet Protocols ("IPs") of Internet content that is either prohibited content or potentially prohibited content under **Schedule 5** of the *Broadcasting Services Act 1992* ("the Act").

### THE REQUEST

4. On 25 February, 2000, Electronic Frontiers requested the ABA for access to a number of documents under the FOI Act. After receiving advice that it was liable to pay charges estimated by the ABA to be $4,400 and after being unsuccessful in its application to have those charges reduced or not imposed, Electronic Frontiers refined the parameters of its request in a letter dated 11 May,

2000. After refinement, it sought, for the period from 1 January, 2000 until the end of February, 2000:

- copies of complaints received under **Part 4** of the *Broadcasting Services Amendment (Online Services) Act 1999*;
- copies of requests made by the ABA to the Office of Film and Literature Classification ("OFLC") for the classification of Internet content;
- classification of Internet content made by the OFLC following a request by the ABA;
- copies of reports concerning interim, final of special take-down notices issued by the ABA;
- copies of blocking requests issued to filtering software manufacturers to add a site or sites to their "*black list*" or to otherwise block access to that site or to those sites by users of their software;
- copies of documents relating to action taken on complaints where a take-down notice was not issued by the ABA i.e. referral to a law enforcement agency. (T documents, pages 243-244 and 232-233)

5. The ABA had made decisions refusing access to certain documents, or passages from certain documents, on the basis of **ss. 37**, **40**, **41** and **43** of the FOI Act. At the hearing, Ms Graham stated that Electronic Frontiers is not seeking access to the names of businesses referred to in the documents sought. Consequently, any claim under **s. 43(1)(c)(i)** need not be considered. Ms Campbell indicated that the ABA had agreed to release the passage naming one of its officers and so no longer relied on **s. 41**.

**THE ABA'S RESPONSE TO THE REQUEST**

6. The ABA identified 175 documents as meeting the description of the documents sought by Electronic Frontiers. Of these, the ABA released 31 in their entirety and 144 in part. In relation to the 144 documents, exemptions from disclosure were claimed in respect of various passages under **ss. 37**, **40**, **41** and **43(1)(c)(i)** of the FOI Act. Since the ABA made its decisions, it has released the information contained in one document which revealed the name of an ABA officer and which it had previously claimed to be exempt under **s. 41**. Electronic Frontiers is

not seeking the names of businesses in relation to which the ABA had claimed exemption under **s. 43(1)(c)(i)**. Those names are revealed in two documents.

7. The remaining documents contain URLs and IPs. That information enables a person to identify and to obtain access to content on the Internet. That content has been found by the ABA to be either prohibited or potentially prohibited under **clauses 30** and **40** of the Act. It is this information that the ABA claims is exempt from disclosure under the FOI Act.

**THE INTERNET**

8. On the basis of the evidence, we have made a number of findings of fact regarding the Internet, its content and its access. We will set them out in this section of our reasons and note that the following 8 paragraphs are based primarily on the evidence of Mr Fraser.

9. We find that the Internet is a world-wide computer network, or network of networks, used to exchange information among the computers connected to it. According to statistics published by the Australian Bureau of Statistics in *Internet Activity Australia* for the December quarter 2000, there were 3.9 million Internet subscribers in Australia as at 30 December, 2000. Of these, 3.5 million were household subscribers and 512,000 were business subscribers. Approximately 95% of all subscribers are connected to the Internet via a modem and telephone line through an Internet service provider ("ISP"). (Exhibit 2, pages112-114)

10. Computers on the Internet are named using domain names based on the organisations to which they belong. So, for example, the domain name aba.gov.au belongs to the ABA and the domain name aat.gov.au belongs to the Tribunal. Generally, each computer on the Internet is assigned a unique address known as an Internet Protocol ("IP") address. The allocation of an IP address is strictly controlled by a limited number of authorities on a geographical basis. The American Registry for Internet Numbers ("ARIN") manages IP address allocation for America, the Carribean and sub-Saharan Africa, Réseaux IP Européens ("RIPE") for Europe, the Middle East and North Africa and the Asia-Pacific Network Information Centre ("APNIC") for the Asia-Pacific region. Domain names are translated to IP addresses using domain name servers.

11. Information on the Internet such as a page on the World Wide Web is known as Internet content. Just as a computer on the Internet is uniquely identified, so too is each piece of Internet content. It is identified by its URL. The URL identifies the protocol used to access the content, or type of content, the computer on which it is located and the location of the computer. Although uniquely identified, the Internet content is not static and may be changed as the content of the Internet site is updated.

12. Content must be hosted on the Internet. Some creators of Internet content host their own Internet content. Most pay an Internet content host to host it on their behalf. In turn, the Internet content host agrees to place the content on a data storage device or server and to make the content available on the Internet. Creators of Internet content are largely free to select their Internet content host.

13. Internet content is portable between Internet content hosts. It is not limited by geographic location as it can be uploaded from one Internet content host in one location to another. A creator of Internet content may choose to move Internet content from one domain to another. Usually, a change of domain will involve a change of part of the URL. Finally, a creator of Internet content may choose to transfer the entire domain on which the content is hosted to a different data storage device, which has a different IP address. If this option is chosen, the new Internet content host must update its domain name server records to ensure that data traffic for the domain and content is routed to the new data storage device. The new Internet content host is able to update its domain server records very quickly and, in any event, within 24 hours. The Internet content can retain its original URL.

14. Newsgroups are a bulletin-board like forum for exchanging information over the Internet. Each group comprises individual postings similar in form to electronic mail messages. Groups are organised in a subject based hierarchy and there are currently more than 30,000 individual groups. The content of newsgroups is stored simultaneously on many Internet content hosts. Most users of the Internet gain access to the content of a newsgroup by means of a data storage device or server operated by their ISP. Generally, each ISP stores only postings from the previous two to seven days in each group. There are, however, World Wide Web

sites, such as http://www.google.com, that also offer access to newsgroup content. Those sites often retain all of the postings and so may be searched by reference to, for example, the author of the posting, its subject and the date on which it was posted.

15. Internet content may be located and access gained to it in a number of ways. The first is to enter the Internet content's URL, when it is known, in the address window of the browser software. For example, entry of http://www.aba.gov.au/what/online/overview/htm in the address window gains access to a page of text from the ABA's web site explaining the co-regulatory scheme for Internet content to be displayed. Entry of http://www.aat.gov.au/decision.htm gains access to a AAT's decisions.

16. The second means of locating and gaining access is through means of a search engine. Knowledge of the URL is not required if a search engine is used. Search engines include "Yahoo!", "Alta Vista" and "Google". Depending on the structure of the search engine, Internet content may be searched by reference to text in the body of a page, the title of a page or the name of a site.

## REGULATION OF THE INTERNET INDUSTRY

### *Powers, functions and responsibilities of the ABA*

17. Among its other responsibilities, the ABA is responsible for monitoring the Internet Industry. That responsibility is given by the Act (**ss. 5(1)(a)** and see also **s. 158(n)**) among whose objects are:

> "*(k) to provide a means for addressing complaints about certain Internet content; and*
>
> *(l) to restrict access to certain Internet content that is likely to cause offence to a reasonable adult; and*
>
> *(m) to protect children from exposure to Internet content that is unsuitable for children; …*" (**s. 3(1)**)

18. To enable the ABA to carry out its responsibility, Parliament has given it a range of functions and powers. They are found in the Act (**ss. 158** and **159**). In relation to the Internet Industry, they were given to the ABA when amendments to the

Act were effected by the *Broadcasting Services Amendment (Online Services) Act 1999* ("Amendment Act"). Those amendments came into operation on 16 July, 1999.

19. In exercising its functions and powers, the ABA is required to use them in a manner that, in its opinion, will:

> "*(i) produce regulatory arrangements that are stable and predictable; and*
>
> *(ii) deal effectively with breaches of the rules established by this Act.*" (**s. 5(1)(b)**)

Where it finds it necessary to use any of its powers to deal with a breach of the Act or of the regulations made under it, the ABA is required to use its powers in a manner that, in its opinion, "*is commensurate with the seriousness of the breach concerned*" (**s. 5(2)**).

***Outline of the Internet regulatory scheme***

20. The Amendment Act introduced a regulatory scheme based upon a model of Internet industry self-regulation within a legislative framework. There are three purposes that regulation is intended to achieve. These were set out in **s. 4(3)** of the Act:

> "*The Parliament also intends that Internet content hosted in Australia, and Internet carriage services supplied to end-users in Australia, be regulated in a manner that:*
>
> *(a) enables public interest considerations to be addressed in a way that does not impose unnecessary financial and administrative burdens on Internet content hosts and Internet service providers; and*
>
> *(b) will readily accommodate technological change; and*
>
> *(c) encourages:*
>
> *(i) the development of Internet technologies and their application; and*
> *(ii) the provision of services made practicable by those technologies to the Australian community; and*
> *(iii) the supply of Internet carriage services at performance standards that reasonably meet the social, industrial and commercial needs of the Australian community.*"

21. The regulatory scheme regarding Online services is set in **Schedule 5** to the Act (**s. 216B**). **Clause 1** of that Schedule sets out the three components comprising the scheme. The first regulates ISPs and Internet content hosts in Australia in relation to Internet content but does not impose any obligations upon the producers of content or the persons who upload content or who have access to content. The second comprises **s. 85ZE** of the *Crimes Act 1914* ("Crimes Act") and State and Territory laws which impose obligations on producers of content and persons who upload content or who have access to content. The third comprises "*a range of non-legislative initiatives*" that are directed towards monitoring content on the Internet and educating and advising the public about content on the Internet.

22. Before looking at the first of the three components in a little more detail, the terms used in **Schedule 5** require some explanation. For the purposes of the Act, an ISP is a person who "*… supplies, or proposes to supply, an Internet carriage service to the public …*" (**cll. 3** and **8(1)**). An "*Internet carriage service*" means a "*… listed carriage service that enables end-users to access the Internet*" (**cl. 3**). What is meant by "*supply to the public*" is set out in **clause 9**:

> "*(2) If:*
>
> *(a) an Internet carriage service is used for the carriage of information between 2 end-users; and*
>
> *(b) each end-user is outside the immediate circle of the supplier of the service;*
>
> *the service is supplied to the public.*
>
> *(3) If:*
>
> *(a) an Internet carriage service is used to supply point-to-multipoint services to end-users; and*
>
> *(b) at least one end-user is outside the immediate circle of the supplier of the service;*
>
> *the service is supplied to the public.*
>
> *(4) If:*
>
> *(a) an Internet carriage service is used to supply designated content services (other than point-to-multipoint services) to end-users; and*
>
> *(b) at least one end-user is outside the immediate circle of the supplier of the service;*
>
> *the service is supplied to the public.*"

23. An "*Internet content host*" is "*… a person who hosts Internet content in Australia, or who proposes to host Internet content in Australia*" (**cl. 3**). "*Internet content*" means:

> "*… information that:*
>
> *(a) is kept on a data storage device; and*
>
> *(b) is accessed, or available for access, using an Internet carriage service*
>
> *but does not include:*
>
> *(c) ordinary electronic mail; or*
>
> (d) *information that is transmitted in the form of a broadcasting service.* (**cl. 3**)

The word "*information*" is given a broad definition to include information in any form, or combination of form, including text, data, speech, music, sounds and visual images (**cl. 3**). In excluding "*ordinary electronic mail*" from the meaning of "*Internet content*", the Act does not intend to exclude a posting to a newsgroup (**cl. 3**).

> "access" *includes:*
>
> "*(a) access that is subject to a pre-condition (for example, the use of a password); and*
>
> *(b) access by way of push technology; and*
>
> *(c) access by way of a standing request.*" (**cl. 3**)

***Internet regulatory scheme – regulation of ISPs and Internet content hosts in relation to Internet content***

24. We will now return to the first of the three components comprising the regulatory scheme. As we have said, it regulates ISPs and Internet content hosts. It does so by focusing on Internet content supplied or hosted, as the case may be, by those ISPs and Internet Content Hosts. In particular, it focuses on "*prohibited content*" and "*potentially prohibited content*". "*Prohibited content*" is defined in terms of whether it is hosted inside or outside Australia:

> "*(1) For the purposes of this Schedule, Internet content hosted in Australia is* ***prohibited content*** *if:*
>
> *(a) the Internet content has been classified RC or X by the Classification Board; or*
>
> *(b) both:*

*(i) the Internet content has been classified R by the Classification Board; and*

*(ii) access to the Internet content is not subject to a restricted access system.*

*(2) For the purposes of this Schedule, Internet content hosted outside Australia is **prohibited content** if the Internet content has been classified RC or X by the Classification Board.*" (**cll. 3** and **10**)

A "*restricted access system*" is a specified access-control system declared as such by the ABA in a written instrument (**cl. 4(1)**). Before making such a declaration, the ABA must have regard to the objective of protecting children from exposure to Internet content that is unsuitable for children and to any other matter that it considers relevant (**cl. 4(2)**).

25. "*Potential prohibited content*" is defined in the following terms:

"*(1) For the purposes of this Schedule, Internet content is **potential prohibited content** if:*

*(a) the Internet content has not been classified by the Classification Board; and*

*(b) if the Internet content were to be classified by the Classification Board, there is a substantial likelihood that the Internet content would be prohibited content.*

*(2) In determining whether particular Internet content is potential prohibited content, it is to be assumed that this Schedule authorised the Classification Board to classify the Internet content.*" (**cll. 3** and **11**)

26. The "*Classification Board*" means that established by the *Classification (Publications, Films and Computer Games) Act 1995* ("Classification Act"). If Internet content consists of the entire unmodified contents of a film or a computer game classified under the Classification Act, that Internet content is taken to have been classified by the Classification Board in the same way under **Schedule 5** (**cl. 12(1)**). If it consists of the entire unmodified contents of a film or a computer game and they have not been classified under the Classification Act, the Classification Board is to classify the Internet content in a way which corresponds with the way in which the film or the game would be classified under the Classification Act (**cl. 12(2)**). If the Internet content does not consist of the entire unmodified contents

of a film or of a computer game, the Classification Board is to classify the Internet content in a way which corresponds with the way in which a film would be classified under the Classification Act (**cl. 13**). In deciding whether or not Internet content consists of the entire unmodified contents of a film, differences between the techniques used to embody sounds and/or visual images in the film and those in a form in which it can be accessed on the Internet are disregarded (**cl. 5**). In certain circumstances, Internet content may be reclassified and provision is made for the review of a classification (**cll. 14** to **21**).

27. The Guidelines were approved by the Commonwealth, State and Territory Censorship Ministers on 18 September, 2000 in accordance with **s. 12(3)** of the Classification Act. The classifications "*R*" and "*X*" mean, respectively, "*restricted to adults 18 years and over*" but the "*X*" rated material is available only for sale or hire in the Australian Capital Territory or in the Northern Territory. In summary, "*Material classified R deals with issues or contains depictions which require an adult perspective*" (Exhibit 3, page 11). The X classification:

> "*… is a special and legally restricted category which contains only sexually explicit material. That is material which contains real depictions of actual sexual intercourse and other sexual activity between consenting adults.*
>
> *No depiction of violence, sexual violence, sexualised violence or coercion is allowed in the category. It does not allow sexually assaultive language. Nor does it allow consensual depictions which purposefully demean anyone involved in that activity for the enjoyment of viewers.*
>
> *Fetishes such as body piercing, application of substances such as candle wax, "golden showers", bondage, spanking or fisting are not permitted.*
>
> *As the category is restricted to activity between consenting adults, it does not permit any depictions of non-adult persons, including those aged 16 or 17, nor of adult persons who look like they are under 18 years. Nor does it permit persons 18 years of age or over to be portrayed as minors.*" (Exhibit 3, page 13)

28. A classification of "*RC*" means that the material has been refused classification and cannot legally be brought into Australia. The Guidelines summarises the criteria for refusing to classify a film or video:

> "*…The criteria fall into three categories. These include films that:*
>
> - *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 be classified RC.*

- *depict in a way that is likely to cause offence to a reasonable adult a person who is or who looks like a child under 16 (whether or not engaged in sexual activity), or;*
- *promote, incite or instruct in matters of crime or violence.*

*Films and videos will be refused classification if they appear to purposefully debase or abuse for the enjoyment of viewers, and which lack moral, artistic or other values, to the extent that they offend against generally accepted standards of morality, decency and propriety.*

*Films and videos will be refused classification:*

*(a) if they promote or provide instruction in paedophile activity;*

*or if they contain:*

*(b) depictions of child sexual abuse or any other exploitative or offensive depictions involving a person who is or who looks like a child under 16;*

*(c) detailed instruction in:*
*(i) matters of crime or violence,*
*(ii) the use of proscribed drugs;*

*(d) depictions of practices such as bestiality;*

*or if they contain gratuitous, exploitative or offensive depictions of:*

*(e) violence with a very high degree of impact or which are excessively frequent, prolonged or detailed;*

*(f) cruelty or real violence which are very detailed or which have a high impact;*

*(g) sexual violence;*

*(h) sexual activity accompanied by fetishes or practices which are offensive or abhorrent;*

*(i) incest fantasies or other fantasies which are offensive or abhorrent.*" (Exhibit 3, pages 14-15)

29. The regulatory scheme, which is administered by the ABA, may be described as both reactive and proactive. It is reactive in the sense that the ABA responds to complaints made to it about prohibited content or potentially prohibited content. It is proactive in the sense that:

"*(1) The ABA may investigate any of the following matters if the ABA thinks that it is desirable to do so:*

*(a) whether an Internet service provider is supplying an Internet carriage service that enables end-users to access prohibited content or potential prohibited content;*

*(b) whether an Internet content host is hosting prohibited content, or potential prohibited content, in Australia;*

*(c) whether an Internet service provider, or an Internet content host:*

*(i) has contravened a code registered under Part 5 of this Schedule that is applicable to the provider or host; or*

*(ii) has contravened an online provider rule that is applicable to the provider or host.*

*(2) Paragraphs (1)(a) and (b) do not authorise the ABA to investigate something that occurs before 1 January 2000."* (**cl. 27**)

30. The steps taken by the ABA when it receives a complaint are summarised in **cl. 2** of **Schedule 5**. After setting out the meaning of "*prohibited content*" *or* "*potential prohibited content*" and the ABA's obligation to investigate a complaint about such content on the Internet, the summary continued:

> "· *If the ABA is satisfied that Internet content hosted in Australia is potential prohibited content, and is likely to be classified RC or X, the ABA must:*
>
> *(a) request the Classification Board to classify the content; and*
>
> *(b) give the relevant Internet content host an* **interim take-down notice** *directing the host not to host the content pending the classification of the content.*
>
> · *If the ABA is satisfied that Internet content hosted in Australia is potential prohibited content, and is likely to be classified R, the ABA must request the Classification Board to classify the content.*
>
> · *If the ABA is satisfied that Internet content hosted in Australia is prohibited content, and is likely to be classified R, the ABA must give the relevant Internet content host a* **final take-down notice** *directing the host not to host the prohibited content.*
>
> · *If the ABA is satisfied that Internet content hosted outside Australia is prohibited content or potential prohibited content, the ABA must:*
>
> *(a) if the ABA considers that the content is of a sufficiently serious nature to warrant referral to a low enforcement agency-notify the content to an Australian police force; and*
>
> *(b) notify the content to Internet service providers so that the providers can deal with the content in accordance with procedures*

*specified in an industry code or industry standard (for example, procedures for the filtering, by technical means, or such content).*

- *Bodies and associations that represent sections of the Internet industry may develop industry codes.*
- *The ABA has a reserve power to make an industry standard if there are no industry codes or if an industry code is deficient.*
- *The ABA may make online provider determinations regulating Internet service providers and Internet content hosts.*" (**cl. 2**)

31. The Internet content host must act in response to an interim take-down notice and must remove the content until the Classification Board has classified it. If, after classification, the content is not prohibited content, the Internet content host may restore the content to its site. If, after classification, the content is prohibited content, the ABA issues a final take-down notice and the content must not be restored. As at the end of February, 2000, the ABA had received 85 complaints. Action following the investigations of those complaints included 18 final take-down notices issued to content hosts in relation to Australian hosted content. On the basis of the paper by Mr Grainger, the Deputy Chairman of the ABA, given on 10 March, 2000, we find that a majority of the notices issued to that time related to content that was classified by the Classification Board as RC. Over 30 items had been referred to the makers of approved filters concerning content hosted overseas. On the basis of the evidence of Mr Fraser, we find that approximately 150 complaints were made to the ABA over the first six months of the scheme's operation. They resulted in the classification of approximately 55 items of Australian hosted content as either RC or X and in approximately 94 of overseas hosted content that would be classified as either RC or X. The number of complaints remained at a similar level in the second six months of the scheme's operation.

32. **Clause 62** of Schedule **5** contemplates the ABA's registering industry codes that have been developed by a body or an association representing a particular section of the Internet industry. Each code that is developed must apply to participants in that section of the Internet industry and must deal with one or more matters relating to Internet activities of those participants. The ABA must be satisfied that the code provides appropriate community safeguards for matters of substantial relevance to the community and deals in an appropriate manner with matters that are not of substantial relevance. It must also be satisfied that, before it was given a copy

of the code, the body or association made a draft copy available for public submissions and for submissions from participants in the section of the Internet industry concerned and considered any submissions it received. The designated body declared under **cl. 58** must have been consulted and the code must be consistent with the relevant provisions of **cll. 59** and **60**.

33. If it considers the development of a code is necessary or convenient in order to provide appropriate community safeguards or otherwise to deal with the performance or conduct of participants in a particular section of the Internet industry and, in the absence of a request, it is unlikely that an industry code would be developed within a reasonable time, the ABA may request a body or association to develop an industry code applying to participants in that section of the Internet industry. The industry code must deal with one or more specified matters relating to the Internet activities of those participants (**cll. 63(1)** and **(2)**). If its request is not complied with or the ABA refuses to register the code that is developed, the ABA may determine a standard in order to provide appropriate community safeguards in relation to the matters specified in its request or otherwise regulate the participants in that section of the Internet industry in relation to those matters (**cl. 68(1)**). The standard determined by the ABA is the industry standard (**cl. 68(2)**). Before determining an industry standard, the ABA must seek public comment and must have due regard to those comments (**cl. 76**). The ABA is also authorised to develop an industry standard where there is no industry body or association (**cl. 69**) or where there is a total failure of industry codes (**cl. 70**) or a partial failure (**cl. 71**).

34. If a person is a participant in a particular section of the Internet industry and the ABA is satisfied that the participant has breached an industry code, it may give the participant a direction under **cl. 66** to comply with that code. A person must comply with that direction which, for the purposes of **Part 6** of **Schedule 5**, is an online provider rule (**cl. 79**). The effect of **cl. 82** of that Part is that, should the person contravene the direction, he, she or it commits an offence. Where an ISP or an Internet content host has contravened an online provider rule (or is doing so), the ABA may give a written direction requiring him, her or it to take specified action directed towards ensuring that the provider or host does not contravene the rule, or is unlikely to do so, in the future (**cl. 83**). Contravention of such a direction is an

offence. The Federal Court may order an ISP or an Internet content host who has acted otherwise in accordance with an online provider rule to cease, as the case may be, supplying the Internet carriage service or hosting that content in Australia (**cl. 85(2)**). It may do so after an application has been made to it by the ABA (**cl. 85(1)**).

35. On the basis of the evidence of Ms Wright, we find that three industry codes, or codes of practice, have been developed by the Internet Industry Association ("IIA"). They are the Content Code 1: ISP obligations in relation to Internet access generally, Content Code 2: (including Schedule 1) ISP obligations in relation to access to content hosted outside Australia and Content Code 3: ICH obligations in relation to hosting of content within Australia (Exhibit 2, pages 1-12). Each code is a module of a Code of Practice. Each was registered by the ABA on 16 December, 1999 and just prior to the commencement of the complaints mechanism on 1 January, 2000.

36. Clause 4.5 of the Code of Practice states that all obligations imposed on Internet content hosts and ISPs in the code are to be interpreted in a manner that is consistent with Parliament's intention set out in **s. 4(3)** of the Act. Among the obligations imposed on the ISP are:

- "*ISPs will take reasonable steps to ensure that Internet access accounts … are not provided to persons under the age of 18 years without the consent of a parent, teacher or other responsible adult. …*" (**cl. 5.1**)

- "*In respect of those of their subscribers who are Content Providers ISPs will:*

  *(a) encourage them to use appropriate labelling systems, in respect of Content which is likely to be considered unsuitable for children according to the National Classification Code, though not Prohibited or Potential Prohibited content; and*

  *(b) inform them of their legal responsibilities, as they may exist under the Act or complementary State or Territory legislation in relation to Content which they intend to provide to the public via the Internet from within Australia..*" (**cl. 5.2**)

- "*ISPs will take reasonable steps to provide users with information about:*

  *(a) supervising and controlling children's access to Internet content;*

*(b) procedures which parents can implement to control children's access to Internet content, including the availability, use and appropriate application of Internet Content filtering software, labelling systems and filtered Internet carriage services.*" (**cl. 5.3**)

- "*ISPs must take reasonable steps to inform their subscribers:*

  *(a) that placing content on the Internet may entail legal responsibilities under applicable State, Territory or Commonwealth law;*

  *(b) about their right to make complaints to the ABA about Prohibited Content or Potential Prohibited Content; and*

  *(c) about the procedures by which such complaints to the ABA can be made.*" (**cl. 5.5**)

- "*ISPs will have procedures in place to deal with complaints from subscribers in respect of unsolicited email that promotes or advertises Internet sites or parts of Internet sites that enable, or purport to enable, end users to access information that is likely to cause offence to a reasonable adult. An ISP shall be deemed to have complied with this provision where they have provided complainants with, or directed them to, information describing methods by which receipt of unsolicited email of this nature can be minimised.*" (**cl. 5.7**)

- "*To the extent applicable, and pursuant to paragraph 60(m) of the Online Services Schedule, an ISP on becoming aware that an Internet Content Host is hosting Prohibited Content in Australia will, provided the ISP is aware of the identity and email address of the Content Host, advise the relevant Content Host by email about the Prohibited Content.*" (**cl. 5.8**)

Content Code 1 also sets out techniques which an ISP may choose to fulfil its obligations. In respect of **cll. 5.2** and **5.3**, it states that:

> "*… ISPs shall be deemed to have fulfilled these requirements where they direct users, by means of a link on their Home Page or otherwise, to resources made available for the purpose from time to time by the IIA, the ABA, NetAlert or other organisation approved by the IIA.*" (**cl. 5.4**)

37. The obligations imposed on ISPs in Content Code 2 are centred on filtering, Approved Filters that are set out in Schedule 1 of the Code of Practice, and a Designated Notification Scheme that is, in brief, the ABA's notification of Prohibited Content or Potential Prohibited Content or information by which they can be identified (**cl. 6.1**). The procedures that ISPs must follow in respect of content

notified under the Designated Notification Scheme depend upon whether subscribers are, or are not, commercial. They are set out in **cl. 6.2** which reads, in part:

> *"(a) ISPs who provide Internet access to subscribers within Australia will as soon as reasonably practicable for each person who subscribes to an ISP's Internet carriage service provide for use, at a charge determined by the ISP, an Approved Filter.*
>
> *…*
>
> *(b) In the case of commercial subscribers, the ISP will, as soon as practicable, provide for use, at a charge and on terms determined by the ISP, such other facility or arrangement that takes account of the subscriber's network requirements and is likely to provide a reasonably effective means of preventing access to Prohibited and Potential Prohibited Content. …*"

**Clause 6.2** does not apply in respect of the supply of Internet carriage services by an ISP where an end user is subject to an arrangement that is likely to provide a reasonably effective means of preventing access to Prohibited Content or Potential Prohibited Content (**cl. 6.4**).

38. In outline and in addition to its statutory obligations, the obligations upon Internet Content Hosts set out in Content Code 3 are:

- "*To the extent applicable, each Internet Content Host will take reasonable steps to ensure that content subscription accounts for content hosted by the Internet Content Host ("subscription accounts") are not provided to persons under the age of 18 years without the consent of a parent, teacher or other responsible adult …*" (**cl. 7.1**)

- "*To the extent applicable Internet Content Hosts will:*

  *(a) encourage Content Providers to use appropriate labelling systems, in respect of Content which is likely to be considered unsuitable for children according to the National Classification Code, though not Prohibited or Potential Prohibited content; and*

  *(b) inform Content Providers of their legal responsibilities, as they may exist under the Act or complementary State or Territory legislation in relation to Content which they intend to provide to the public via the Internet from within Australia.*" (**cl. 7.2**)

- "*To the extent applicable, Internet Content Hosts will take reasonable steps to provide users with information about:*

  *(a) supervising and controlling children's access to Internet content;*

  *(b) procedures which users including parents and others responsible for children can implement to control access to Internet content,*

*including the availability, use and appropriate application of Internet Content filtering software, labelling systems and filtered Internet carriage services.*" (**cl. 7.3**)

- "*Internet Content Hosts will take reasonable steps, for example through the inclusion of a relevant term of the relevant hosting contract or an acceptable use policy, to inform Content Providers for whom hosting services are provided by the Internet Content Host not to place on the Internet content in contravention of any State, Territory or Commonwealth law.*" (**cl. 7.5**)

- "*To the extent applicable, Internet Content Hosts will take reasonable steps to inform users about:*

  *(a) their right to make complaints to the ABA about Prohibited Content or Potential Prohibited Content; and*

  *(b) procedures as determined by the ABA by which users can make complaints to the ABA about Prohibited Content or Potential Prohibited Content.*" (**cl. 7.6**)

- "*To the extent applicable, Internet Content Hosts will have procedures in place to deal with complaints from subscribers in respect of unsolicited email that promotes or advertises Internet sites or parts of Internet sites that enable, or purport to enable, end users to access information that is likely to cause offence to a reasonable adult. An Internet Content Host shall be deemed to have complied with this provision where it has provided complainants with, or directed them to, information describing methods by which receipt of unsolicited email of this nature can be minimised.*" (**cl. 7.8**)

- "*When an Internet Content Host has been given a notice under the Act by the ABA that is hosting on a web server or other content database within its control and within Australia, material which is deemed by the ABA to be Prohibited Content or Potential Prohibited Content:*

  *(a) the Internet Content Host must, within the timeframe required under the Act:*

    *(i) remove that Content from the Web Site or database;*

    *(ii) in the case of R-rated content which is not subject to a restricted access system, apply to it such a system; or*

    *(iii) take any other action provided for under the Act in relation to the notice; and*

  *(b) upon doing so, the Internet Content Host must, where applicable, inform the customer who placed that content on the Internet Content Host's Web Site or database that the customer's conduct is a breach of the customer's service conditions.*" (**cl. 7.9**)

- *"To the extent applicable, and pursuant to paragraph 60(m) of the Online Services Schedule an Internet Content Host, on becoming aware that another Internet Content Host is hosting Prohibited Content in Australia will, provided the first Internet Content Host is aware of the identity and email address of the second Content Host, advise the second Content Host by email about the Prohibited Content."* (**cl. 7.11**)

For the purposes of **cl. 7.6**, Internet Content Hosts are deemed to have taken reasonable steps:

> "*… where they have included a relevant term or statement in any hosting contract with end-users, any acceptable use policy, a notice on the Internet Content Host's Home Page, a link to the information on a Web Page approved by the IIA for that purpose.*" (**cl. 7.7**)

39. Pursuant to **cl. 92**, an application may be made to the Tribunal for review of a number of decisions including a decision to give an Internet content host an interim or final take-down notice, a request to the Classification Board to classify Internet content hosted in Australia by an Internet content host or a decision to give an Internet service provider or an Internet content host a direction under either **cll. 66** or **83**.

***Internet regulatory scheme – legal obligations in Commonwealth and State laws***

40. The second component of the regulatory scheme are the legal obligations imposed by **s. 85ZE** of the *Crimes Act* and by State and Territory laws upon producers of content and persons who upload or access content. **Section 85ZE** provides:

> *"**Improper use of carriage services***
>
> *(1) A person must not intentionally use a carriage service supplied by a carrier:*
>
> *(a) with the result that another person is menaced or harassed; or*
>
> *(b) in such a way as would be regarded by reasonable persons as being, in all the circumstances, offensive.*
>
> *Penalty: Imprisonment for 1 year."*

41. The *Censorship Act 1996* (WA) ("WA Censorship Act") prescribes offences in relation to objectionable and restricted material. "*Objectionable material*" is defined to mean:

> "*(a) a film classified RC, a computer game classified RC, or a refused publication;*
>
> *(b) child pornography;*
>
> *(c) an article that promotes crime or violence, or incites or instructs in matters of crime or violence; or*
>
> *(d) an article that describes or depicts, in a manner that is likely to cause offence to a reasonable adult –*
>
> *(i) the use of violence or coercion to compel any person to participate in, or submit to, sexual conduct;*
>
> *(ii) sexual conduct with or upon the body of a dead person;*
>
> *(iii) the use of urine or excrement in association with degrading or dehumanizing conduct or sexual conduct;*
>
> *(iv) bestiality;*
>
> *(v) acts of torture of the infliction of extreme violence or extreme cruelty.*" (**s. 99**)

"*Restricted material*" is defined to mean:

> "*… an article that a reasonable adult, by reason of the nature of the article, or the nature or extent of references in the article, to matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena, would regard as unsuitable for a minor to see, read or hear.*" (**s. 99**)

42. Subject to the exemption of certain articles and computer services by the Censor or the Minister (W.A) (**s. 105**), the offences in relation to objectionable material and restricted material are:

> "*101(1) A person must not use a computer service to –*
>
> *(a) transmit an article knowing it to be objectionable material;*
>
> *(b) obtain possession of an article knowing it to be objectionable material;*
>
> *(c) demonstrate an article knowing it to be objectionable material;*
>
> *(d) advertise that objectionable material is available for transmission; or*
>
> *(e) request the transmission of objectionable material knowing it to be objectionable material.*

*Penalty:*

*(a) in the case of an individual, $15000 or imprisonment for 18 months;*

*(b) in any other case, $75000.*

*(2) It is a defence to a charge of an offence against this section to prove that the article concerned is –*

*(a) an article of recognized literary, artistic or scientific merit; or*

*(b) a* bona fide *medical article,*

*and that transmitting, obtaining possession of, demonstrating, advertising, or requesting the transmission of, the article is justified as being for the public good.*

*102(1) A person must not use a computer service to transmit restricted material to a minor.*

*Penalty:*

*(a) in the case of an individual, $5000 or imprisonment for 6 months;*

*(c) in any other case, $25000.*

*(2) A person must not use a computer service to make restricted material available to a minor.*

*Penalty:*

*(a) in the case of an individual, $5000 or imprisonment for 6 months;*

*(b) in any other case, $25000.*

*(3) It is a defence to a charge of an offence against subsection (1) or (2) to prove that –*

*(a) the defendant complied with a code of practice;*

*(b) the defendant took all reasonable steps in the circumstances to avoid a contravention of the subsection; or*

*(c) the defendant believed on reasonable grounds that –*

*(i) the person to whom the defendant transmitted the restricted material was not a minor; or*

*(ii) the restricted material would not be made available to a minor."*

43. In addition, the WA Censorship Act provides that a person must not possess or copy an unclassified film that would, if classified, be classified RC and must not possess or copy a film classified RC (**s. 81**).

44. The *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995* (ACT) makes similar provision when it provides in **s. 24** that except for the purposes of classification or law enforcement, a person shall not

possess a film classified RC or an unclassified film with the intention of selling or exhibiting the film and shall not copy such a film.

45. **Section 74** of the *Classification (Publication, Films and Computer Games) Enforcement Act 1995* (Tas) provides that a person must not have possession of a child abuse product or a bestiality product and **s. 72** provides that a person must not make or reproduce such a product or be involved in that making or reproduction. The relevant terms are defined in **s. 71**:

> "'***bestiality product***' *means a publication, film or computer game that depicts in pictorial form bestiality;*
>
> *'child abuse product' means a publication, film or computer game that describes or depicts a person (whether engaged in sexual activity or otherwise) who is, or who looks like, a child in a manner that is likely to cause offence to a reasonable adult;*
>
> *'make' includes print, photograph and record.*"

46. The *Classification of Publications, Films and Computer Games Act* (NT) ("NT Classification Act") defines "*objectionable material*", "*restricted material*" and "*code of practice*" and creates offences in the same terms as in **s. 101** of the WA Censorship Act (**ss. 50Z**, **50ZA** and **50X**). The *Classification (Publication, Films and Computer Games) (Enforcement) Act 1995* (Vic) ("Victorian Classification Act"), takes a slightly different approach. It defines the following terms:

> "'***material unsuitable for minors of any age***' *means --*
>
> *(a) objectionable material; or*
>
> *(b) a film that is classified R or would, if classified, be classified R; or*
>
> *(c) a publication that is classified Category 1 restricted or Category 2 restricted, or would, if classified, be classified Category 1 restricted or Category 2 restricted;*
>
> *'***material unsuitable for minors under 15***' means --*
>
> *(a) a film that is classified MA or would, if classified, be classified MA; or*
>
> *(b) a computer game that is classified MA (15+) or would, if classified, be classified MA(15+);*
>
> *'***objectionable material***' means --*
>
> *(a) an objectionable publication; or*
>
> *(b) an objectionable film; or*
>
> *(c) a computer game that --*

(i) *depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that it offends against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that it should not be classified; or*

(ii) *describes or depicts a person who is, or looks like, a minor under 16 engaging in sexual activity or depicted in an indecent sexual manner or context; or*

(iii) *promotes, incites or instructs in matters of crime or violence; or*

(iv) *is unsuitable for a minor to see or play; or*

(v) *is classified RC or would, if classified, be classified RC." (**s. 56**)*

The Victorian Classification Act provides for the following offences:

*"58(1) A person must not use an on-line information service to publish or transmit, or make available for transmission, to a minor material suitable for minors of any age.*

*Penalty:*

*(a) if the material is objectionable material--240 penalty units or imprisonment for 2 years;*

*(b) in any other case--60 penalty units or imprisonment for 6 months.*

*(2) It is a defence to a prosecution for an offence against sub-section (1) to prove that--*

*(a) the defendant--*

*(i) did not know and could not reasonably have known that the person to whom the material was published or transmitted or made available for transmission was a minor; and*

*(ii) had taken reasonable steps to avoid publishing transmitting, or making available for transmission, the material to a minor; or*

*(b) the defendant believed on reasonable grounds that the material was not material unsuitable for minors of any age.*

*(3) Sub-section (1) does not apply to a person who provides an on-line information service or a telecommunication service unless the person knowingly publishes, transmits or makes available for transmission to a minor material unsuitable for minors of any age.*

*(4) A person must not use an on-line information service to publish or transmit, or make available for transmission, material to a minor under 15 knowing it to be material unsuitable for minors under 15.*

*Penalty: 30 penalty units.*

*(5) It is a defence to a prosecution for an offence against sub-section (4) to prove that--*

*(a) the defendant believed on reasonable grounds that the parent or guardian of the minor had consented to the material being published or transmitted, or made available for transmission, to the minor; or*

*(b) the defendant--*

*(i) did not know and could not reasonably have known that the person to whom the material was published or transmitted, or made available for transmission, was a minor under 15; and*

*(ii) had taken reasonable steps to prevent publishing or transmitting, or making available for transmission, the material to a minor under 15.*

*(6) Sub-section (4) does not apply to a person who provides an on-line information service or a telecommunication service unless the person knowingly publishes, transmits or makes available for transmission to a minor under 15 material unsuitable for minors under 15.*

*59 A person must not--*

*(a) publish an advertisement or notice; or*

*(b) transmit, or make available for transmission, on an on-line information service an advertisement or notice; or*

(c) *knowingly allow an on-line information service to be used for publishing or transmitting, or making available for transmission, an advertisement or notice—*

*that objectionable material is available for on-line computer access.*"

47. On the basis of the evidence of Ms Wright, we find that the ABA has negotiated Memoranda of Understanding ("MOUs") with the police services in New South Wales, Queensland, Victoria, Tasmania and Victoria concerning the exchange of information about "*sufficiently serious*" Internet content. Further MOUs are being negotiated with the police services in the Northern Territory and South Australia. On the basis of Mr Grainger's paper, we find that as at 10 March, 2000 when he wrote that paper, four complaints had been referred to law enforcement agencies for investigation (Exhibit B, page 5).

***Internet regulatory scheme – monitoring, education and advice***

48. The third component of the regulatory scheme comprises the ABA's monitoring, educating and advisory roles. These are specified in greater detail in **cl. 94** of Schedule 5:

"*(a) to monitor compliance with codes and standards registered under Part 5 of this Schedule;*

*(b) to advise and assist parents and responsible adults in relation to the supervision and control of children's access to Internet content;*

*(c) to conduct and/or co-ordinate community education programs about Internet content and Internet carriage services, in consultation with relevant industry and consumer groups and government agencies;*

*(d) to conduct and/or commission research into issues relating to Internet content and Internet carriage services;*

*(e) to liaise with regulatory and other relevant bodies overseas about co-operative arrangements for the regulation of the Internet industry, including (but not limited to) collaborative arrangements to develop:*

*(i) multilateral codes of practice; and*

*(ii) Internet content labelling technologies;*

*(f) to inform itself and advise the Minister on technological developments and service trends in the Internet industry."*

49. On the basis of Ms Wright's evidence, we find that the ABA reports to Parliament each six months on the operation of the regulatory scheme. In addition, information regarding the ABA's operations are directly available to the public through its Annual Report and on its website. Pursuant to **cl. 95** of **Schedule 5**, the Minister must have a review of the operation of that Schedule before 1 January, 2003. The Code of Practice would be reviewed in June, 2001 with industry and public consultation.

50. Also on the basis of Ms Wright's evidence, we find that Australia has been an associate member of INHOPE (i.e. the Internet Hotline Providers in Europe), which is an international body of hotlines, since September, 2000. It previously enjoyed observer status. Hotlines that are qualified for membership must have mechanisms for formally investigating complaints made to them by members of the public regarding Internet content. Members are encouraged to have formal relations with both industry bodies and law enforcement agencies. INHOPE currently has 11 members in the form of three German hotlines, two hotlines from the Netherlands and a hotline from each of Holland, England, the Irish Republic, Austria, Denmark, Sweden and Spain. Its three associate members are an Australian hotline operated by the ABA, a Norwegian hotline operated by Save the Children and the American Cybertip line operated by the National Centre for Missing Children. The operators of the 14 hotlines variously represent government, industry and community and child welfare groups.

51. Members and associate members of INHOPE refer Internet content to the member hotline for the country in which that material is hosted. If a member receives a complaint about Internet content hosted in its own country, it would investigate that complaint and liaise with law enforcement and industry bodies as required. Details of such matters as the URL on the Internet content will not be released to other members. If, however, a member receives a complaint about Internet content hosted in the country of another member, that member will send to that other member details of the complaint and of the URL. To date, several thousand such referrals have taken place. The type of material referred includes child pornography, extreme violence, depictions of sexual violence and Nazi propaganda.

**THE EVIDENCE**

***Locating prohibited content and potentially prohibited content***

52. Mr Fraser said in his affidavit:

> "*38. In my experience, prohibited and potential prohibited content can be easily located using a search engine to search by the name of a site or the title of a page of content. For example, I looked at a sample of the content falling within the ambit of this Freedom of Information ('FOI') application and assessed the ease with which the content could be located on a search engine, using the URL, site name, page title or details of a newsgroup posting as the search terms.*
>
> *39. In a number of cases I found that the actual piece of content that was dealt with in an investigation was among the list of possible matches returned by the search engine. In nearly all cases, a significant number of links to potential prohibited content were returned in the search. Without the URL address, IP address, site name, page title or description of content access to prohibited content or potential prohibited content would be pretty much 'hit and miss'.*" (Exhibit 4)

53. In cross-examination, Mr Fraser explained that, if the ABA considers that content is likely to be classified R by the Classification Board, it does not issue an interim take-down notice. It advises the Internet content host that it has asked for classification but the host is not required to remove the content. If the ABA investigates content hosted outside Australia and forms the view that it would be likely to be classified R if classified by the Classification Board, it is not required to notify the filtering software manufacturers. The scheme does not attempt to prevent

access to content that is hosted outside Australia and that would be classified R in Australia. There are other measures that are part of the scheme, Mr Fraser said, that advise people about managing their access to content that would assist them to restrict their access to R rated content. Such measures include, for example, the installation of filters. He agreed that "*You could say that*" it is "*parents' responsibility to manage their children's access in terms of R rated material on overseas sites*" (transcript, page 45).

54. In cross-examination, Mr Fraser explained how, in his view, a person could gain access to content taken down from an Australian site and moved to an overseas site. It could retain its IP address with .com.au retained in that address even though it is now hosted outside Australia. It could be moved with a different IP address. He said that information such as page titles and site names can be used on search engines to locate content even if the IP address is not known. Mr Fraser agreed with Ms Graham that there is a large quantity of content on the Internet that is accessible, that is potentially prohibited and that has not been investigated by the ABA.

55. Mr Fraser was asked to consider the case in which the ABA receives a complaint about content appearing on a News Group. That content has been accessed through the complaint's ISP and the ISP and the complainant are both in Australia. Should the OFLC's classification result in its being prohibited content, Mr Fraser said that the ABA does not issue a take-down notice to every ISP in Australia providing access to the News Group postings. For the purpose of the investigation, he said, the Internet content host is considered to be the person's ISP and the ABA is required to issue the take-down notice to that Internet content host. The ABA does not issue take-down notices to other ISPs who carry the News Group and the content.

***The nature of the content complained about***

56. In Mr Grainger's paper, he said that a majority of the 18 take-down notices issued to content hosts in relation to Australian hosted content "*…relate to content that was classified 'RC' (Refused Classification) by the Classification Board (predominantly content of a sexual nature with 'underage connotations').*" (Exhibit B, page 5). That was the position to the end of February, 2000 but Ms Wright said that,

as time has gone by, the ABA has noticed a movement away from complaints about Australian hosted material to an increasing emphasis on complaints about overseas hosted material. The majority of more recent complaints are concerned with depictions of child pornography or with depictions of children that would be classified RC by the Classification Board.

57. Ms Wright said that the ABA and the OFLC have, from time to time, undertaken research to ascertain the public's understanding of the classifications given to film and video. She said that the research concluded that a classification of "M" advises of a medium level of violence and has meaning for the public. The public understands that the classification will have the same meaning whether it is ascribed to a video at the video store or to a film shown on television or at the cinema. The Guidelines were reviewed in 2000. There is to be a review of the computer games guidelines but some of the material in computer games is appearing in the medium of DVD and that has led to consideration being given to bringing the guidelines in relation to all media into line.

***Nature of information in documents for which exemption is claimed in part***

58. Mr Fraser agreed with Ms Graham that some of the material for which exemption is claimed has not been classified either RC or X. Some have been classified below the R level. The material in the documents, Mr Fraser said, is closely related to content which was found to be prohibited content or was likely to be classified as RC or X or, in the case of Australian hosted content, at the R level. "*Closely related*", Mr Fraser said, means that the documents contained text which could possibly enable a person to locate the material in other documents, which have been classified and which contain prohibited content. For example, the documents containing content that was not prohibited may have similar URLs, similar page titles or other information likely to lead a person to content that is prohibited content on that site.

***Consequences of revealing URLs and IPs***

59. If URLs, IPs, IP addresses, page titles or the descriptions of Internet content were released to the public, Mr Fraser said:

" *… there is a real likelihood that an end-user with this information would be able to quite easily access the exact content determined by the ABA to be prohibited or potentially prohibited content.*

*41. I also believe that if content which was the subject of a take-down notice had been moved overseas and retained its original URL address an end user would easily be able to access the prohibited content by simply typing in the URL address into the address line of the browser.*

*42. In instances where the content which was subject of a take-down notice has been moved overseas and the URL has been amended, information such as page titles, description of content could be used by an end-user to quite easily locate the content investigated by the ABA.*

*43. Content which was the subject of a take down notice would also be accessible if an end-user does not have an updated scheduled filter installed.*

*44. Release of the URL addresses sent to makers of scheduled filters would similarly enable end-users to access prohibited content if they do not have an approved filter installed or if they do, it has not been updated.*" (Exhibit 4)

60. Referring to Mr Fraser's affidavit and the ABA's responsibilities set out in **s. 3** of the Act, Ms Wright set out her reasons for considering that disclosure of the information sought in this case would undermine the effectiveness of the regulatory scheme:

"*38. The operations of the ABA are designed to minimise the possibility of the Australian community obtaining access to prohibited content and potential prohibited content as set out in the BSA. The effectiveness of the ABA's take-down notice would be substantially adversely affected if any of the URL addresses, IP addresses, descriptions of content, site names or page titles were disclosed, resulting in the content taken down being able to be accessed on an overseas or different domestic site. I refer to the affidavit of Richard James Fraser sworn 14th of June 2001, in particular paragraphs 36-44 in which he describes the way in which information regarding URL addresses, IP addresses, descriptions of content, site names or pages titles can be used to access material on the Internet.*

*39. There is no way in which the ABA could alter its operations to prevent users with this information from obtaining such access. Nor would the ABA be able to prevent the URL address from being moved to another site.*

*40. Locating sites hosting prohibited content and potential prohibited (sic) can be time consuming and not always easy to find. I refer to the affidavit of Richard James Fraser sworn 14th of June 2001, in particular paragraph 39 where he states that without the URL address, IP address, site name, page title or description of content access to*

*prohibited content or potential prohibited content would be pretty much 'hit and miss'.*" (Exhibit 2)

61. Ms Wright noted that no person has sought to exercise the right under **cl. 92** to have reviewed the ABA's decisions to classify Internet content, to issue notices or to give directions. A classification decision may be reviewed by the Classification Board and no person has sought that review. In her oral evidence, Ms Wright said that URLs and other information identifying the site on which the material appears is not sent to the Classification Board when it is sent for classification. At the moment, classification decisions regarding that material is not disclosed on the OFLC's data base. Protocols are being negotiated between the ABA and the OFLC as to the manner in which the material is to be referred to and captured. Material is sent from the ABA to the OFLC by secure link and both have indemnity from any prosecution that could otherwise arise as a result of that transfer. With regard to the manner in which the OFLC notifies classification decisions on its web site, Mr Fraser said that the OFLC and the ABA have agreed on a format that does not contain information likely to lead a person to the prohibited content. Each item will contain a very short description of the type of content and possibly a date on which it was classified.

62. In her oral evidence, Ms Wright said that all ISPs and Internet content hosts have promptly complied with take-down notices. When asked by Ms Graham whether the ABA could order the ISP or Internet content host not to publish that content elsewhere and particularly overseas, Ms Wright replied that the ABA could not have any influence over that publication unless it were brought to its attention and it would act through its overseas protocols. Ms Wright said that, were the material to be moved to an overseas Internet content host, it could still use the same URL address including the .au. If the URL were released, therefore, it could still be accessed. Her concern was expressed in the following passage of her oral evidence:

"*… I'm expressing a concern that the more people who have access to material that relates to prohibited material that directly enables you to find it, the more chances are increased that it will be accessed. I refer to colleagues in INHOPE who said that they had requests to release that information, but because the security of that information has never been able to be categorically guaranteed, they have not released it and that would be my concern as well. Further to that, my previous experience at the OFLC means*

*that when material may for any period look as if it has been refused classification and is made illegal if that material, for example, is then overturned by the Review Board distributors love that because they know people are drawn to have a look. So I think there is the chance that the material you cannot guarantee the security and the idea of forbidden fruit draws people to it so I have a concern there.*" (transcript, pages 27-28)

63. Ms Wright expressed the following views on the effect of disclosure under the FOI Act:

> "*43. I am of the view that these mechanisms provide a comprehensive and effective accountability regime and that the public interest ground favouring disclosure is of less weight. I believe that the industry and the public are satisfied with how the scheme has been administered so far. The fact that no affected party has sought to exercise their review rights supports this belief. It is difficult to conceive how government accountability could be advanced by placing in the public domain details of prohibited and potentially prohibited content which could enable the public including children to access illegal or unsuitable content. I consider that the public interest in preventing access to illegal or unsuitable content as per the intention of Parliament greatly outweighs any public interest arguments raised by the EFA in favour of release of the information exempted by the ABA in this freedom of information application.*
>
> *44. Release of the information would contribute to easier access to content intended to be restricted or prohibited under the BSA. The release of the URL addresses sent to makers of approved filters (regarding content hosted overseas) is even more problematic in that it could have the effect of creating an* 'Australian black list' *that would be of interest to paedophiles internationally. Such an outcome would be in direct conflict with the public policy behind the amendments to the BSA, which led to the introduction of Schedule 5 of the Act. It is also my belief that it would make INHOPE member hotlines reluctant to forward online child pornography that is hosted in Australia to the ABA for investigation if there was the possibility of the URL's contributing to such a list.*
>
> *45. Access under FOI to the ABA list sent to makers of approved filters setting out URL addresses of prohibited content could also have the undesirable effect of assisting end-users to commit a criminal offence under State and Territory legislation. For example, possession of child pornography, is a criminal offence under the following Acts:*
>
> Crimes Act 1900 (A.C.T), s92NB;
>
> Crimes Act 1958 (VIC), s70
>
> Crimes Act 1900 (N.S.W), s578B
>
> Censorship Act 1996 (W.A.), s60(4)
>
> Summary Offences Act 1958 (S.A.), s33(3)

*46. Possession of material which if classified under the National Classification Code would be RC, is a criminal offence under the following Acts:*

Censorship Act 1996 (W.A), s60, s81

Classification (Publication, Films and Computer Games) Enforcement Act 1995 (TAS), s74

*47. Exhibition and sale of X-rated and R-rated material to children under 18 is prohibited under various State and Territory Classification legislation.*

*48. Use of a computer to obtain possession, transmit or demonstrate objectionable material (that is material likely to fall within the RC classification) would also be a criminal offence under: the* Censorship Act 1996 (WA)*, see section 101 and 102; the* Classification of Publications, Films and Computer Games Act (NT) 1998*, see sections 50X, 50Z and 50ZA; and the* Classification (Publications, Films and Computer Games) (Enforcement) Act 1995 (VIC)*, see sections 56, 57 and 58.*

*49. Further, when considering whether to release the information exempted by the ABA in this matter, it is important for a decision maker to keep in mind that RC, X or R rated material may be accessible in certain instances even though a content host has complied with a take-down notice. Prohibited content could be accessed if a site has moved offshore and retained its '.au' domain name or where an end-user does not have an updated scheduled filter installed and therefore would still be able to access the content at the same URL. The release by a decision maker of URL addresses for example, could therefore have the undesirable consequence of enabling end-users to commit offences under State legislation.*

*50. I believe that disclosure of information exempted by the ABA in this matter such as URL addresses of prohibited content or potential prohibited content or descriptions of such content, would be contrary to Parliament's intention to have a consistent legal environment as disclosure without any restraint on its use would allow the information to be placed in the public domain and would enable end-users to access content which the Commonwealth and State and Territories have legislated against such access or possession.*" (Exhibit 2)

64. In giving oral evidence, Ms Wright said that agencies concerned with child welfare, child abuse, child pornography or paedophilia will, from time to time, forward information to the ABA's hotline regarding information with which they have concerns. In her view, Ms Wright said, such agencies would seriously consider whether they should forward such information if its URLs were to be released under the FOI Act. That would follow from their seeing potential access to the Internet content as further abuse of the child victims depicted within the material. Such

agencies would look to the ABA for guarantees that it will not release such information to anybody other than those who must have it in order to discharge their duties.

65. Mr Fraser was asked in cross-examination regarding what would happen if he and his unit were not to receive complaints with URLs or site names or if the numbers of complaints were to be substantially reduced. He said that the regulatory scheme is complaint-based so that the cessation or reduction of complaints would lead to the cessation of, or reduction in, the effectiveness of the scheme. In addition, it would compromise the ABA's role in advising and assisting parents in relation to prohibited content and potential prohibited content and in relation to parents' supervising their children's access to the Internet. The ABA's relationship with overseas bodies and particularly with INHOPE member hotlines would be jeopardised if information were released to the public. Those member hotlines would be unlikely to share complaint information with the ABA if it were subsequently to be released to the public.

66. Later, he said that a reduction in the number of complaints would significantly undermine the ABA's credibility as the Internet content regulator and undermine the public's confidence in the scheme. It would do that if their complaints about child pornography, for example, were to lead to the release of details of the site. It might be seen as simply promoting, rather than restricting, access to it.

67. When asked in cross-examination about the manner in which a release of information about overseas material would undermine the ABA's scheme, Mr Fraser replied that:

> "*I would say that the objects of the Act are reasonably clear in requiring the ABA to take steps to prevent people from accessing content that's harmful to children or otherwise offensive. In terms of the ABA's specific functions it would also, I think, run contrary to the ABA's efforts to advise and assist parents and carers of children in that releasing that information would effectively be promoting it or would sort of be otherwise drawing attention to it whereas on the other hand the ABA is sort of advising people about the steps they can take to limit access to that.*" (transcript, page 46)

If those people were using an approved filter, they would not be able to gain access to either prohibited content or potentially prohibited content.

68. Mr Fraser agreed with Ms Graham that the ABA could not force the filtering software manufacturers to update their filters to take account of the ABA's take-down notices but added that they would be removed from the list of Approved Filters set out in Schedule 1 of the Code of Practice. When the ABA classifies content hosted in Australia as either R, X or RC, it does not always notify manufacturers of Approved Filters. If the ABA becomes aware that the content has been moved overseas, it will do so and that has happened in a number of cases. In response to Ms Graham's question as to why it did not notify those manufacturers in case Australian hosted content is moved overseas, Mr Fraser said that the Act sets out the steps that the ABA must take. It must be satisfied that the content is hosted outside Australia in order to notify manufacturers of Approved Filters in accordance with the processes in the Code of Practice.

***ABA's interaction with INHOPE***

69. Ms Wright said that the ABA has gained the confidence of members and associate members of INHOPE while it had attended its meetings as an observer. Consequently, they are more likely to refer material to the ABA and such referrals have occurred from the National Centre for Missing Children since September, 2000. The majority of complaints received by the ABA would not, however, be from INHOPE hotlines.

70. Ms Wright said that the ABA would never send R rated material to another hotline to investigate because, under the Act, it would not investigate such material unless it received a complaint. Each country defines the characteristics of the material that is of concern to it. Some overseas hotlines do investigate sexual material. Referrals from members and associate members of INHOPE were counted among the 85 complaints received to 10 March, 2000. The ABA has done so as it has the power to investigate matters of its own volition.

71. Ms Wright said that INHOPE has stated clearly that it would not forward Internet content to the ABA for investigation and would not receive information from it were the ABA unable to guarantee that URLs or information identifying prohibited content or potentially prohibited content would not be unconditionally released to the public.

**LEGISLATIVE FRAMEWORK**

72. **Section 11(1)** of the FOI Act provides that:

> "*Subject to this Act, every person has a legally enforceable right to obtain access in accordance with this Act to:*
>
> *(a) a document of an agency, other than an exempt document; or*
> *(b) an official document of a Minister, other than an exempt document.*"

73. It is clear from the terms in which the right is couched that it is a qualified right. The first qualification is that it is a right to have access to a "*document of an agency*" or to "*an official document of a Minister*". In so far as an agency is concerned, that means that the right is access to a document in the possession of the agency (**s. 4(1)**). The word "*document*" is defined in very broad terms:

> "*(a) any of, or any part of any of, the following things:*
>
> *(i) any paper or other material on which there is writing;*
>
> *(ii) a map, plan, drawing or photograph;*
>
> *(iii) any paper or other material on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them;*
>
> *(iv) any article or material from which sounds, images or writings are capable of being reproduced with or without the aid of any other article or device;*
>
> *(v) any article on which information has been stored or recorded, either mechanically or electronically;*
>
> *(vi) any other record of information; or*
>
> *(b) any copy, reproduction or duplicate of such a thing; or*
>
> *(c) any part of such a copy, reproduction or duplicate;*
>
> *but does not include:*
>
> *(d) library material maintained for reference purposes; or*
>
> *(e) Cabinet notebooks;*" (**s. 4(1)**)

The terms of the definition are broad enough to encompass within them records kept on paper and in electronic form such as in e-mail records or in documents kept in

electronic form. They are broad enough to encompass drawings and graphs as well as records of text or script.

74. The words "*Subject to this Act*" appear in **s. 11** for a person's right is qualified by other provisions of the FOI Act. Those sections include **ss. 12** and **13** (excluding access to certain categories of documents), **24** (permitting certain workload factors to be taken into account in refusing a request) and **24A** (permitting a request to be refused if a requested document cannot be found or does not exist). None is relevant in this case. Apart from these qualifications, **s. 11** is explicit in its terms that the right of access is not to every document of an agency. It is only to every document in the possession of that agency that is not an "*exempt document*". In so far as an agency is concerned, an "*exempt document*" is a document that is exempt by virtue of a provision of **Part IV** of the FOI Act (**s. 4(1)**).

75. Two sections in **Part IV** are relevant: **ss. 37(2)(b)** and **40(1)(d)**. Beginning with **s. 37(2)(b)**, it provides that:

> "*A document is an exempt document if its disclosure under this Act would, or could reasonably be expected to:*
> *(a)* …
>
> *(b)* *disclose lawful methods or procedures for preventing, detecting, investigating, or dealing with matters arising out of, breaches or evasions of the law the disclosure of which would, or would be reasonably likely to, prejudice the effectiveness of those methods or procedures;* …
>
> (d) …"

76. **Section 40(1)(d)**, provides that:

> "*Subject to subsection (2), a document is an exempt document if its disclosure under this Act would, or could reasonably be expected to:*
>
> *(a)* …
> *(b)* …
> *(c)* …
> *(d)* *have a substantial adverse effect on the proper and efficient conduct of the operations of an agency;*
> *(e)* …"

**Section 40(2)** adds a rider to the exemption created by **s. 40(1)**. Its effect is that a document that would otherwise be exempt under **s. 40(1)** is not exempt if its disclosure would, on balance, be in the public interest.

**CONSIDERATION**

77. Before considering the particular claims for exemption made on behalf of the ABA, we want to make three general observations. The first relates to the nature of some of the information that may be encompassed within some of the documents captured by Electronic Frontier's request. Some of that information may lead a person to content on the Internet that is not only rated R, X or RC, in the case of Australian hosted content, or X or RC, in the case of overseas hosted content, but may, in some instances but not all, contain material that depicts child pornography, paedophilia or child abuse. That there is such content on the Internet and that it is capable of being accessed by users of the Internet is of grave concern. It is of grave concern should such material or material that otherwise comes within the R, X or RC classifications be accessed by young persons whom every reasonable adult would want to protect from it. It is also of grave concern if material classified RC were to depict, for example, images of child pornography, paedophilia or child abuse. Reasonable adults do not condone those who seek to view such material. There are also concerns that their viewing such material repeats and perpetuates the abuse that those depicted in the material have already suffered.

78. The second relates to issues of censorship. Comparisons and contrasts can be drawn between what happens in the classification of film and video and what is said to be the position in relation to Internet content. In relation to the former, it is said, it is possible to know the material that is prohibited from being brought into Australia and so prohibited from being shown in Australia i.e. those films and videos that are colloquially said to be "banned". Although described as classification, this amounts to censorship of what the Australian public may see and of what it may bring into Australia. The public will have means to know what it is not permitted to see. Should a member of the Australian public wish to see the film or video, then he or she knows what it is and may seek it out overseas and view it overseas according to the laws of that overseas country. Those who do are able to form a view as to the manner in which the material that they may not see is assessed by reference to the standards

set out in the Guidelines. They form a view as to whether the standards are being applied too rigorously. If they are thought to have been applied too leniently, that no doubt would be a matter already canvassed in Australia in public debate. That debate would have been conducted on the basis that the film and video material had been classified and so was available to be viewed. If the material were not classified and so not permitted to be viewed in Australia, many people would not, when they were outside Australia, want to take advantage of any opportunity (lawful or otherwise) to see film and video banned in Australia. The fact that an opportunity may assist to view film or video outside Australia could, however, be said to ensure the integrity of the classification system by ensuring that it is never open to abuse and used for purposes other than classification according to the Guidelines.

79. In contrast, if the URLs and IPs are exempt under the FOI Act then this effectively means that the Australian public may not know what it may not see. As a consequence, no member of the public has the opportunity to view the material at any time. That lack of opportunity born of a veil of non-disclosure could bring into question whether take-down notices are issued only in relation to Internet content that is prohibited content or potentially prohibited content and so bring into question the integrity of the scheme under the Act. We should say that we have no reason to question, and do not question, the integrity of the ABA. What we do say is that secrecy may of itself undermine the public's confidence. This was a matter addressed during the Second Reading debate (Hansard, Senate, 25 May, 1999, page 5271 (Exhibit A)).

80. Our third general comment relates to the scheme that is established under the Act and brings us to the manner in which we have undertaken the review of the ABA's decision. It seems to us that some of the evidence and particularly that given in cross-examination is directed to the effectiveness of the scheme of regulation of Internet content. Questions were raised, for example, as to how effectively the scheme protects children from gaining access to Internet content when the children's parents may choose, and lawfully choose, not to install an Approved Filter in order to block content hosted on an overseas site. There were questions as to how effectively it does so when the ABA does not consistently advise filtering software manufacturers of Internet content that it has investigated on overseas sites and that would be rated R

if located on an Australian site. There were questions as to how effectively it could do so when it could not require the manufacturers of Approved Filters to upgrade their software to take account of take-down notices issued to Internet content hosts and to ISPs. All that it could do was remove them from the Schedule of Approved Filters. There are also questions as to how effectively any scheme may effectively regulate access to Internet content that may be easily charged and readily moved from one ICH to another.

81. These are all issues of concern and matters that no doubt require ongoing debate and consideration. We will return to them later in these reasons but, for the moment, they are not relevant in considering whether disclosure of the URLs and IPs under the FOI Act would have the effect described in **s. 40(1)(d)**. In order to carry out that task, we must take the scheme established by the Act as it is. Beginning with **s. 40(1)(d)**, therefore, we must ask whether disclosure of the URLs and IPs would, or could reasonably be expected to, have a substantial adverse effect on the operations of the ABA. One of the functions of the ABA is to implement the scheme under the Act and so the first question is whether disclosure would, or could reasonably be expected to, have a substantial adverse effect on the operations of the scheme under the Act.

82. Beginning with **s. 40(1)(d)**, the words "*would, or could reasonably be expected to*" have been considered in cases such as *Attorney-General's Department v Cockcroft* (1986) 64 ALR 97 (Bowen CJ, Sheppard and Beaumont JJ). Bowen CJ and Beaumont J said in considering the same expression used in **sub-paragraph 43(1)(c)(ii)**:

> "*In our opinion, in the present context, the words 'could reasonably be expected to prejudice the future supply of information' were intended to receive their ordinary meaning. That is to say, they require a judgment to be made by the decision-maker as to whether it is reasonable, as distinct from something that is irrational, absurd or ridiculous, to expect that those who would otherwise supply information of the prescribed kind to the Commonwealth or any agency would decline to do so if the document in question were disclosed under the Act. It is undesirable to attempt any paraphrase of these words. In particular, it is undesirable to consider the operation of the provision in terms of probabilities or possibilities or the like. To construe s 43(1)(c)(ii) as depending in its application upon the occurrence of certain events in terms of any specific degree of likelihood or probability is, in our view, to place an unwarranted gloss upon the relatively plain words of*

*the Act. It is preferable to confine the inquiry to whether the expectation claimed was reasonably based (see* Kioa v Minister for Immigration & Ethnic Affairs *(1985) 62 ALR 321 per Gibbs CJ and Mason J.*" (page 106)

83. The expectation must be of "*a substantial adverse effect*" on the proper and efficient conduct of ABA's operations. The words "*substantial adverse effect*" have been considered in a number of cases and were set out in a previous decision, *Re Bayliss and Department of Health and Family Services* (AAT 12277, 10 October, 1997) (Deputy President Forgie):

"*40. The phrase 'substantial adverse effect', and in particular the word 'substantial', have been considered in a number of cases. The word 'substantial', is not one of clear meaning. There are at least two alternative senses in which it may be used, on the one hand it may mean large or weighty or of considerable amount, on the other, it may mean real or of substance as opposed to nominal or illusory. In Palser v. Grinling (1984) 1 All ER 1 Viscount Simon held that in the context in which he had to consider it the word 'substantial' meant 'considerable, solid or big'.*

*41. In Tillmanns Butcheries Pty Ltd v. Australasian Meat Employees Union & Ors (1979) 27 ALR 367 Bowen CJ and Deane J considered the words 'substantial loss or damage'. Bowen CJ at page 374 said:*

> *'The word 'substantial' would certainly seem to require loss or damage that is more than trivial or minimal. According to one meaning of the word the loss or damage would have to be considerable (see Palser v. Grinling [1984] AC 291 at 316-7). However, the word is quantitatively imprecise; it cannot be said that it requires any specific level of loss or damage. No doubt in the context in which it appears the word implores a notion of relatively, that is to say, one needs to know something of the circumstances of the business affected before one can arrive at a conclusion whether the loss or damage in question should be regarded as substantial in relation to that business.'*

*42. Deane J at page 382 said:*

> *'The word 'substantial' is not only susceptible of ambiguity; it is a word calculated to conceal a lack of precision. In the phrase 'substantial loss or damage', it can, in an appropriate context, mean real or of substance as distinct from ephemeral or nominal. It can also mean large, weighty or big. It can be used in a relative sense or can indicate an absolute significance, quantity or size … As at present advised, I incline to the view that the phrase, substantial loss or damage, in s45D(1) includes loss or damage that is, in the circumstances, real or of substance and not insubstantial or nominal. It is, however, unnecessary that I form or express any concluded view in that regard, since the ultimate conclusion which I have reached is*

*the same regardless of which of the alternative meanings to which reference has been made is given to the word 'substantial' in s45D(1).'*

*43. In Harris v Australian Broadcasting Corporation and Others (1983) 50 ALR 551, Beaumont J considered whether reports of an independent review of the Legal Department of the respondent were exempt within the meaning of paragraph 40(b) of the Act. Beaumont J said that it is possible that the reports could embarrass those charged with supervising or reviewing the operations of the Legal Department but went on to say on page 564:*

> *'However, I am not persuaded that any such effect, even if adverse, could fairly be described as 'substantial' in its impact. In my view, the insertion of a requirement that the adverse effect be 'substantial' is an indication of the degree of gravity that must exist before this exemption can be made out.'*

*Beaumont J was considering section 40 as it existed before it was replaced in 1983. The particular words which he considered, however, have not been varied and are still relevant.*

*44. Muirhead J has also considered the expression 'substantial adverse effect' as it appears in section 40 in the case of Marco Ascic v Australian Federal Police (1986) 11 ALN N184. Muirhead J considered the passage from the Harris case to which I have referred above and said:*

> *'The reference to 'gravity' in that dictum (and I say so with respect) causes me some difficulty. 'substantial' is a word of common usage which can stand on its own feet and the word ascribed to it in statutory interpretation will depend on the statute and of course the issues under consideration. Deane J gave detailed consideration to the word in Tillmanns Butcheries Pty Ltd v. Australasian Meat Industry Employees' Union (1979) 27 ALR 376 at 382. Whilst the court there was considering an application under s. 45D of the Trade Practices Act which refers to 'substantial loss or damage' his Honour's words that 'substantial loss or damage … includes loss or damage that is in the circumstances, real or of substance and not insubstantial or nominal' appear to me to be appropriate to most circumstances and closer to the plain meaning of the word and its dictionary interpretations.' (page N185)*

*45. This Tribunal, presided over by Beaumont J, has considered paragraph 40(1)(c) in Re Williams and Registrar of the Federal Court of Australia (1985) 8 ALD 219 (Mr McMahon, then Senior Member and Dr Renouf, Member). Beaumont J said at page 222 that the difficulties in establishing that 'substantial adverse effects' will occur are formidable. This was referred to by the Tribunal in Re Dyrenfurth and Department of Social Security (1987) 12 ALD 577 (Deputy President Todd, Senior Member Balmford and Mr Cohn, Member). The Tribunal said:*

> *'If we had been approaching the present matter in, as it were, a vacuum, we might have been tempted to think that the difficulties were not so formidable. But the fact is that the practice of the respondent agency is stated to be what we might call a generous one. We have already set out the agency's guidelines. It is perfectly true that in general terms this Tribunal is not bound by an agency's guidelines, but that is not the point here. We are uncertain to what extent they are applied (see T26), but they exist as a fact, and their existence in that form seems to us to undermine the suggestion of substantial adverse consequence.' (page 585)*
>
> *46. Finally, I will refer to the conclusion adopted by the Tribunal in Re Thies and Department of Aviation (1986) 9 ALD 454 (Deputy President Thompson, Senior Member Hallowes and Mr Trinick, Members) that a 'substantial adverse effect' 'connotes an adverse effect which is sufficiently serious or significant to cause concern to a properly informed reasonable person' (page 463).*
>
> *47. … It seems to me that the ordinary meaning of the words 'substantial adverse effect' leads to a conclusion that something more than 'concern' is required before the adverse effect can be said to be a substantial adverse effect. Concern may be generated by matters of many differing degrees of gravity. What is required by the exemption in paragraph 40(1)(d) is made out is an adverse effect that is real or of substance and not that which is insubstantial or nominal. That is consistent with the judgements of Federal Court in Ascic and in Tillmans Butcheries by both of which I am bound.*"

We note that this was also the interpretation of the words "*a substantial adverse effect*" adopted by Deputy President McMahon in *Re Connolly and Department of Finance (1994) 34 ALD 655*.

84. The substantial adverse effect must be on the "*proper and efficient operations of the agency*". It seems to us that **s. 40(1)(d)** uses the word "*operations*" in this context in its ordinary meaning. That meaning is:

> "…***4a*** *An act of a practical or technical nature,* esp. *one forming a step in a process. …* ***b*** *…Also, a business concern or enterprise…*" (The New Shorter Oxford English Dictionary, 3rd edition, 1993)

In *Re James and Australian National University* (1984) 2 AAR 327, the Tribunal considered **s. 40(1)(d)** in the context of a request for documents recording lecturers' comments in student record sheets together with the names of examiners of honours theses and their tentative grades. Deputy President Hall said that:

> "*As a matter of ordinary English I think that the expression 'the conduct of the operations of an agency' is capable of extending to the way in which an agency discharges or performs any of its functions. So construed, I agree with Mr Toper that it is capable of extending to the discharge by the University of its academic functions in relation to the awarding and conferring of degrees and diplomas (see s. 6 of the* Australian University Act *1946 (Cth))*."
> (pages 340-341)

This passage was expressly approved by the Full Court of the Federal Court in *Searle Australia Pty Ltd v Public Interest Advocacy Centre and Another* (1992) 16 AAR 28 (Davies, Wilcox and Einfeld JJ) (page 32).

85. In the case with which we are concerned, the scheme set out in **Schedule 5** of the Act is concerned with regulating access to Internet content hosted in Australia. It does not do so by attempting to regulate those who create the content or those who may view the content but by regulating those who host it (the Internet content hosts) and those who provide the means of gaining access to it (the ISPs). In the case of Internet content hosts, **Schedule 5** of the Act does so directly by requiring them to remove content from their sites if the ABA issues a take-down notice, whether interim, final or special. In the case of ISPs, the Act does so indirectly through the Code of Practice formulated according to **Schedule 5**.

86. On the basis of the evidence of Ms Wright and Mr Fraser and on our own examination of the scheme set out in **Schedule 5** of the Act and the Code of Practice, we find that the ABA's administration and implementation of the scheme is dependent, to a significant degree, upon its receiving complaints about Internet content rather than upon, for example, its monitoring the Internet or undertaking some other form of investigation. Its reliance upon complaints is clear from the Act itself in so far as the regulation of Internet content hosts in Australia is concerned. That is the first component of the scheme. In that case, the complaints may come from any source including members of the public. Under **Schedule 5** it is required to act upon complaints about Internet content. Indeed, complaints are at the heart of the scheme of regulation of Internet content hosts established in the Act.

87. Complaints are not expressly at the heart of the second component of the scheme i.e. the legislative obligations imposed by Commonwealth and State laws on the producers of content and persons who upload or access content. Part of that

second component, though, is the ABA's requirement to liaise with law enforcement agencies about Internet content that is "*sufficiently serious*" Internet content. It has already negotiated MOUs with the police services in New South Wales, Queensland, Victoria, Tasmania and Victoria concerning the exchange of information about "*sufficiently serious*" Internet content and is negotiating further MOUs with the police services in the Northern Territory and South Australia. Implicit in its obligations to refer "*sufficiently serious*" Internet content is that it has become aware of such content. In view of the way in which we have found the scheme works, it follows that complaints must play some considerable role in enabling the ABA to identify the material it then refers.

88. The ABA's membership of INHOPE is part of the implementation of the third component. Based on the evidence of Ms Wright, we find that INHOPE members refer Internet content to other member countries in which the content is hosted. That content comes to the attention of INHOPE members in the first place through complaints made to them.

89. In view of the operation of each component of the scheme under the **Schedule 5**, we have concluded that complaints are an integral part of its effective operation. Without those complaints, the ABA would not be able to carry out its functions under **Schedule 5** to refer the content complained about to the Classification Board or to issue take-down notices. Its ability to refer "*sufficiently serious*" content to law enforcement agencies would be substantially hampered for the Internet content that may come within that description will not be referred to it.

90. On the basis of the evidence of Ms Wright and Mr James, we are satisfied that it is reasonable to expect that, should the IPs and URLs of Internet content that is potentially prohibited content or prohibited content be revealed to the public, the number of complaints will be substantially reduced. That would follow from the perception, rightly or wrongly, that the list of IPs and URLs would encourage certain people to seek access to the Internet content complained about. We are satisfied that there is a reasonable likelihood that, once known, it is reasonably likely that such access could be gained even if a take-down notice has been issued to the Internet content host as it is reasonably likely that the Internet content could be moved to an overseas site. On the basis of the evidence of Ms Wright, who has

attended meetings of INHOPE and who has communicated with its members regarding the revelation of URLs and IPs, we are also satisfied that it is reasonable to expect that INHOPE members will not refer to the ABA complaints about Internet content that they have received if URLs and IPs are publicly revealed.

91. In view of the conclusion we have already reached regarding the integral role played by complaints in the administration of the scheme and in the effectiveness of that administration, we are satisfied that revelation of the URLs and IPs to the public would, or could reasonably be expected, to have a substantial adverse effect on the ABA's ability to administer the scheme under **Schedule 5** either properly or efficiently. As administration of the scheme is one of the ABA's functions, we are satisfied that disclosure would, or could reasonably be expected to, have a substantial adverse effect on the proper and efficient conduct of its operations. Therefore, the URLs and IPs are exempt under **s. 40(1)(d)** of the Act.

92. That brings us to **s. 40(2)**. Would the disclosure of the URLs and the IPs be, on balance, in the public interest? The authorities on this aspect of the provision were considered in *Re Booker and Department of Social Security* (AAT 6189, 13 September 1990) (Deputy President Forgie) when it was said:

> "*41. That leaves for consideration sub-section 40(2). The relationship between sub-section 40(2) and sub-section 40(1) is identical to that between sub-section 33A(5) and sub-section 33A(1). These latter provisions, which deal with matters of Commonwealth/State relations and information communicated by a State to the Commonwealth, were considered by the Federal Court (Woodward, Wilcox and Burchett JJ) in* Arnold (on behalf of Australians for Animals) v. Queensland & Anor *(1987) ALR 73 at 607. Wilcox J at pages 616-617 said:*
>
> > "Finally, it is important to bear in mind the significance of sub-s(5) in the scheme of s33A. Sub-section (5) assumes that, as a general principle, there is a public interest in the non-disclosure of a document falling within sub-s(1). But it contemplates that, nonetheless, it may, on balance, be in the public interest for matter in that document to be disclosed. The sub-section does not specify criteria for consideration in the making of that judgment. All relevant circumstances must be taken into account. One of those circumstances will always be the principle enshrined in s3 of the Act. ... It will be noted that Parliament was not content merely to espouse a policy of extending access to information, as stated in s3(1). The legislature went further by requiring the implementation of that policy, as far as possible, in the exercise of the discretions conferred by the Act. Although it would not

> be correct to regard s33A(5) as conferring a discretion, the command of s3(2) is an indication that Parliament regarded the principle constituting a weighty factor to be taken into account in making a judgment as to the public interest in any decision whether to disclose particular documents. In a particular case, especially where the degree of public disadvantage caused by disclosure is small, or the prospect of any public disadvantage is comparatively remote, that principle may itself be enough to tip the balance in favour of disclosure, notwithstanding that the information falls within s33A(1)."
>
> *Burchett J (with whom Woodward J agreed) said at page 627:*
>
> "Reference has also been made to sub-s(5) of s33A which provides: *'This section does not apply to a document in respect of matter in the document the disclosure of which under this Act would, on balance, be in the public interest.'* That sub-section does not confer a discretion upon anyone. It requires a determination of a matter of fact, albeit a matter upon which different minds might well, in a particular case, reach different conclusions. Where either branch of sub-s(1) is found to apply, what sub-s(5) does is raise the question whether nevertheless it can be affirmed of matter in the document that its disclosure under the Act would, on balance, be in the public interest. In reaching that determination, it is clear that the tribunal would have regard to the object of the Act expressed in s3, but it would also have regard to the provision by Parliament of the exemption. It might be expected in practice to look for special features of the instant case which might indicate where, in that particular case, the balance lay. Parliament having provided an exemption, and an escape route from that exemption, I do not think it is very profitable to put a gloss upon the terms which Parliament has itself laid down as a test to be applied - it is for the decision maker to decide whether he can affirm on balance that disclosure would in the public interest.'"

93. In this case, it seems to us that we must have regard to a number of factors. One is the object of the FOI Act to "…*extend as far as possible the right of the Australian community to access to information in the possession of the Government of the Commonwealth…*" (FOI Act, **s. 3(1)**). Another is the scheme of regulation established by the Act in relation to Internet content. Behind both factors are other factors some of which are reflected in the general observations we made at the beginning of this section of our reasons. Those observations raise important issues relating to censorship, openness of government and even to the confidence that the public has in the agencies of government to implement and administer its schemes with integrity for secrecy can ultimately lead to the public's questioning integrity even where there is no need for such questioning. They also raise questions as to the effectiveness of the scheme to carry out the objects identified in **s. 3(1)(k)**, **(l)** and **(m)** of the Act.

94. In addition, there are questions raised by Ms Graham regarding the development of filters to stop material that it is illegal for adults to possess. She submitted that the technology could be developed but that it was impossible to do so given what she described as "*the ABA's regime of secrecy*".

95. We have already found that disclosure would, or could reasonably be expected to, have a substantial adverse effect on the proper and efficient management of the scheme and so on the operations of the ABA. That is the scheme through which Parliament seeks to achieve the objects set out in **ss. 3(1)(k)**, **(l)** and **(m**) of the Act. Among those is an important object of protecting children from exposure to Internet content that is regarded as unsuitable for them. It appears on its face that it may be an imperfect scheme but perhaps that is to be expected given the practical difficulties in regulating a medium that is more nebulous than film or print and in the context of very difficult social and technological issues. For all that, it is the scheme that Parliament has chosen and it is the only statute based scheme in existence at the moment. To undermine its effectiveness, as we consider is reasonably likely to happen were we to release the requested URLs and IPs, would be not only to take away its foundation but also to take away the effectiveness of steps taken voluntarily by parents to make use of an Approved Filter. That would follow from the ABA's reduced effectiveness in identifying content of which the filter software manufacturers are advised.

96. We have found the issues in this case to be of some difficulty. We have no reason to think that Electronic Frontiers seeks the information for anything other than the most honourable reasons. The use of the information in order to develop more sophisticated filters seems to be a worthwhile and proper use. The difficulty that we have is that a person's right of access is not affected by his or her reasons for seeking it (FOI Act, **s. 11(2)(a)**). Access granted under the FOI Act must be considered as access to the world at large and the fact that Electronic Frontiers seeks it for a legitimate and indeed worthy purpose does not give it any greater right than a person who may seek it for reasons that are not legitimate and worthy.

97. Taking all of these matters into consideration, we have concluded that disclosure under the FOI Act would not, on balance, be in the public interest within

the meaning of **s. 40(2)**. On this occasion, considerations favouring its disclosure are outweighed by the substantial adverse effect that we consider would result from disclosure. We note that the scheme is to be reviewed before 1 January, 2003 and would hope that the review is able to incorporate issues of the type that have faced us in this case.

98. It follows that we have concluded that the documents sought are exempt pursuant to **s. 40(1)(d)** in so far as they reveal URLs and IPs. In view of that conclusion, we do not need to consider the ABA's claim that the documents are also exempt under **s. 37(1)(b)**.

99. For the reasons we have given, we affirm the decision of the respondent dated 6 September, 2000 affirming its earlier decision dated 21 July, 2000.

I certify that the ninety-nine preceding paragraphs are a true copy of the reasons for the decision herein of Miss S A Forgie (Deputy President),

Signed: ……..

Paul Paczkowski Associate

| | |
|---|---|
| Dates of Hearing | 18 and 19 July, 2001 |
| Date of Decision | 12 June, 2002 |
| For the Applicant | Ms Graham |
| For the Respondent | Ms Campbell |