

FEASIBILITY STUDY

ISP LEVEL CONTENT FILTERING

FEBRUARY 2008

Report Prepared By:

Louise Collins
Peter Love
Dr Bjorn Landfeldt
Peter Coroneos

On behalf of the Internet Industry Association (IIA)

i. INTRODUCTION

In September 2007, the Australian Government commissioned a feasibility study into implementation of ISP level content filtering, where all ISPs would be required to provide a filtered Internet service for families who prefer this protection option. This report outlines the results of the study.

The report is divided into four parts:

Part 1: Main report

- Containing the study background, methodology, results and recommendations.

Part 2: Attachments

- Acknowledgements & Roles
- Background & Methodology (detailed version)
- Bibliography
- Dictionary of Terms
- Questionnaire - Survey of Australian Internet Service Providers
- Detailed Questionnaire Results
- ISP Feedback
- Organisations Contacted
- Profiled ISP List
- Legal Risk Assessment of the Three ISP Level Filtering Models
- Technical Filtering Techniques
- ACMA Blacklist
- Report from Independent Technical Specialist
- Profile of Personnel Involved in this Study

Part 3 International Survey

- This is a detailed international study on international trends and practices related to ISP level filtering. Elements of this report have been utilised in Part 1.

PART 1

MAIN REPORT

TABLE OF CONTENTS – MAIN REPORT

PART 1	4
MAIN REPORT	4
1.0 EXECUTIVE SUMMARY	8
1.1 <i>Key Findings</i>	8
1.2 <i>Recommended Next Steps</i>	13
SECTION A: BACKGROUND AND METHODOLOGY	14
1.0 Project Background	15
2.0 Project Objectives	15
3.0 Terms of Reference	15
4.0 Limitations	16
5.0 Approach	17
5.1 <i>Secondary Research</i>	17
5.2 <i>Primary Research</i>	18
5.3 <i>Expert Opinion</i>	18
SECTION B: SECONDARY RESEARCH RESULTS	19
1.0 ISP Industry Profile.....	20
1.1 <i>Total Number of Internet Household Subscribers</i>	20
1.2 <i>Size Categorisation of ISPs</i>	20
2.0 Content Provider Profile.....	22
3.0 Related Australian Studies	23
3.1 <i>CSIRO, Blocking Content on the Internet: a Technical Perspective, 1998</i>	23
3.2 <i>CSIRO, Effectiveness of Internet Filtering Software Products, 2001</i>	24
3.3 <i>Ovum Report, Internet Content Filtering, 2003</i>	24
3.4 <i>RMIT, A Study on Server Based Internet Filters: Accuracy, Broadband Performance Degradation and some Effects on the User Experience, 2006</i>	25
SECTION C: PRIMARY RESEARCH RESULTS.....	26
1.0 Management Models For ISP Filtering	27
3. Qualitative Data from Face-to-face Interviews and Focus Groups	32
2.1 <i>ISPs</i>	32
2.2 <i>Content Providers</i>	36
2.3 <i>Filter Vendors</i>	39
2.3.1 Filter Vendor Technologies	40
2.4 <i>Industry Associations</i>	41
2.5 <i>International ISPs and Overseas Regulatory Bodies</i>	42
3.0 Quantitative Data from Questionnaire.....	44
3.1 <i>Questionnaire Results</i>	44

3.1.1	Retail ISP Responses	44
3.1.2	Wholesale Service Provider Responses	45

SECTION D - FILTERING IMPLEMENTATIONS, AUSTRALIA AND OVERSEAS..... 46

1.0	Filtering Implementations.....	47
1.1	<i>International Implementations</i>	47
1.1.1	Denmark	47
1.1.2	Finland	47
1.1.3	Germany	47
1.1.4	Ireland	48
1.1.5	Italy	48
1.1.6	Norway	48
1.1.7	Sweden	48
1.1.8	United Kingdom	49
1.1.9	Canada	49
2.0	Australian Implementations	50
2.1	<i>Webshield</i>	50
2.2	<i>ItXtreme</i>	52

SECTION E - TECHNICAL ASSESSMENTS..... 53

1.0	Filtering Classification Methods	54
1.1	<i>ACMA blacklist</i>	54
1.2	<i>Vendor-maintained blacklists</i>	55
1.3	<i>Dynamic Analysis</i>	56
1.4	<i>Strategic Implications</i>	57
2.0	Category-Based Filtering	58
2.1	<i>System Aspects of Content Filtering</i>	58
2.1.1	Importance of Aims and Policy	58
2.1.2	Technical Considerations of Content Classification	58
2.2	<i>Stopping Prohibited Content in the Internet</i>	59
2.2.1	Impact of IP address and domain blocking	59
2.2.2	Impact of richer multimedia	60
3.0	Technical aspects of Dynamic Content Filtering	61
3.1	<i>Overview of Dynamic Content Filtering</i>	61
3.2	<i>Methods for content classification</i>	61
3.3	<i>Adversary actions and implications</i>	62

SECTION F: INDEPENDENT LEGAL REVIEW..... 64

1.0	Independent Legal Assessment of Management Models	65
1.1	<i>Differences between models</i>	65
1.1.1	Government	65
1.1.2	ISPs	65
1.1.3	Users	65
1.1.4	Outsourced service providers	65
1.2	<i>Service Specific Risks</i>	66
1.2.1	Possession/distribution of illegal content	66
1.2.2	Over-blocking and under-blocking	66
1.2.3	Service degradation and breach of existing ISP contracts	66
1.2.4	Interception and hacking	67
1.2.5	Freedom of expression	67

1.2.6	Privacy	67
1.2.7	Negligence	68
1.2.8	Misleading conduct	68
1.2.9	Sale of goods and provision of services	68
1.2.10	More general issues	68
SECTION G: CONSOLIDATION		69
SECTION H: ISSUES & RECOMMENDED NEXT STEPS		78
1.0	Issues for consideration	79
1.1	<i>Possession and distribution of illegal content</i>	79
1.2	<i>Technical Solution</i>	79
1.3	<i>Management Models</i>	81
1.4	<i>Filtering – what to filter, how to maintain it</i>	82
1.5	<i>Legal</i>	85
1.6	<i>Social</i>	88
1.7	<i>Compliance and Auditing</i>	89
1.8	<i>Financial</i>	90
1.9	<i>Customer support</i>	92
1.10	<i>Anti-Competitive Practices</i>	93
2.0	Recommended Next Steps	93

TABLE OF FIGURES

Figure 1.0: Profile of ISP Industry by Customer Base	21
Figure 2.0: Third Party Managed Model	28
Figure 3.0: ISP Managed Model	29
Figure 4.0: Hybrid Managed Model	31
Figure 5.0: ACMA Blacklist Classification Process	55
Figure 6.0: Vendor Blacklist Classification Process	56
Figure 7.0: Classification Speed Vs Accuracy - ACMA Blacklists, Vendors Blacklists, Dynamic Analysis	57
Figure 8.0: Video Content Trend	60

TABLE OF TABLES

Table 1.0: No. of Large/Very Large ISPs	20
Table 2.0: Geographic Distribution	22
Table 3.0: Technology Type	22
Table 4.0: Coverage	22

1.0 EXECUTIVE SUMMARY

The scope of this study is vast and encompasses a large variety of parameters, such as the operational, legal, technical and financial aspects of ISP filtering. A key assumption of the study is that a content filtering system must provide the capacity for end users to opt-in, and by inference, opt-out of the filtering capability. Many stakeholders were involved in the study, including: ISPs, content providers, filtering system vendors, authorities/regulators, industry associations, and overseas organisations with direct experience of ISP level filtering.

The study was conducted as follows:

- The existing body of knowledge was researched through the collection of available reports from previous Australian and international studies. In addition, the project team visited and interviewed organisations in countries that have implemented content filtering schemes.
- In order to understand the composition of the Australian ISP industry, data was collected from the Internet Industry Association (IIA), the Australian Bureau of Statistics (ABS) and the Telecommunications Industry Ombudsman (TIO).
- Face-to-face interviews and focus groups were held to enable a direct dialogue with the ISP industry.
- A questionnaire was developed and specific input sought nationally from the ISP industry.
- Face-to-face interviews were also held with content producers, filter vendors and industry associations to capture the views and concerns from this group of stakeholders.
- Independent expert legal opinion was commissioned from a law firm specialising in telecommunications.
- Independent technical expertise was commissioned from Sydney University.

1.1 Key Findings

The study highlights six 'Key Findings' that are summarised below.

In the key findings mention is made of both a national filtering scheme and a national filtering service. We have defined them as follows:

National Filtering Scheme: A scheme where ISPs provide a filtered Internet service for Internet users.

National Filtering Service: A filtering capability that is managed externally from the ISP, by an approved third party.

Key Finding 1

There is a need for a clear policy on the goals of any filtering system that might be implemented.

From many perspectives, the feasibility of any system implementation depends on what is to be achieved. The importance of having a clear objective is reflected in the comment below:

“Any analysis of mechanisms needs to be done in the context of the overall goal; without knowing what the expectations/goal is it's very hard to make valid assertions on how well a mechanism will work.” (Source: CISCO Systems 2007)

It should be stated from the outset that there is always a technically savvy person who will be motivated to circumvent any and all filtering mechanisms. As such there is consensus among the stakeholders that it is extremely difficult to stop undesirable content from being accessed on the Internet. However, goals such as inhibiting the inadvertent access to undesirable content - like child pornography - by the unmotivated user, are much more likely to be achieved.

Having a clear objective will lead to the development of an appropriate solution and an understanding of the likely consequences of such a solution. Some things to consider when coming up with an objective are:

- What types of users are to be filtered (e.g. average users, or the technically savvy and motivated)?
- Will filtering be optional?
- What content is intended to be blocked?
- Does the filtering need to be consistent; i.e. the same for every ISP?
- Will businesses be required to implement filtering?

As an example, the following objectives were outlined in Sweden's national filtering scheme:

- To stop accidental access (protect customers);
- To restrain recruitment of new consumers of illegal images;
- To assist in preventing the sexual exploitation of children; and
- To remove any financial incentive to produce child abuse images.

The Internet Watch Foundation in the United Kingdom has the following objectives for its web content filtering program:

- Reduce the occasions when innocent Internet users might be exposed to traumatic and unlawful images;
- Diminish the re-victimisation of children by restricting opportunities to view their sexual abuse; and
- Disrupt the accessibility and supply of such content to those who may seek out such images.

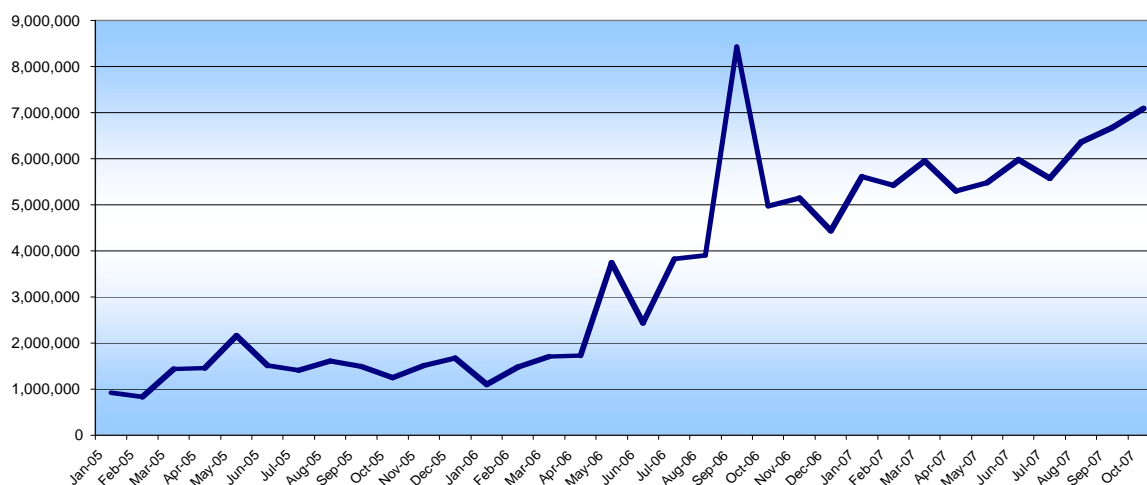
Key Finding 2

The focus of the study was on content available in the form of web pages on the World Wide Web. This does not fully reflect the current dynamics of Internet based media.

Video streaming has grown enormously over the last 18 months. Video streaming requires high-speed broadband capability. This growth in video streaming has serious implications for the performance and feasibility of content filtering – particularly filtering that uses any type of dynamic analysis (also refer to **Key Finding 6**).

**Video Content Streaming
Usage trends for Period Jan '06 - Oct
'07**

(Source: Digital Content Provider, Name Supplied)



The above figure shows the trend in video streaming requests from an Australian content provider. As can be seen, usage of video as a media format is increasing rapidly.

Every minute, eight hours of video is uploaded on to YouTube (Source: Google Australia). This makes scanning of content prior to posting virtually impossible.

In addition, there are numerous realms on the Internet, other than 'web pages', that are popular ways of making content available. These include peer-to-peer networks that enable file sharing, chat forums such as MySpace, and instant messaging services such as MSN, Skype and Yahoo.

Key Finding 3

Australia has a very heterogeneous ISP industry. Depending on the nature of a mandated filtering function, the impact on industry may be significant.

The Australian ISP industry contains over 770 businesses (this number based on TIO statistics as of 23 November 2007). The industry has a small number of large players. Only 32, or 4.1% of the total number of ISPs, have more than 10,000 customers. Of this top 32 only nine have more than 100,000 customers. Approximately 738 ISPs in Australia have fewer than 10,000 subscribers. Lower subscriber numbers usually mean smaller margins, and hence a reduced capacity to put in place complex filtering

capabilities. Primarily because of resources, infrastructure and capital constraints. As per the agreed scope, the study did not incorporate mobile internet service providers. This market segment should be included in future studies.

Key Finding 4

The industry is not well prepared for the implementation of content filtering systems. Our findings show that there is great disparity in the vision of how such systems should be implemented and the perceived level of difficulty in implementation.

As part of the study, three possible management models for content filtering systems were developed for the focus groups and the questionnaire.

- Model 1. The ISP-based model, where *the filtering function and customer support are an integrated part of the ISPs own infrastructure* and daily operation functions. Thus, in this model, the ISP independently manages all aspects of the system.
- Model 2. The third-party model, *where the filtering function and customer support are managed by an external party*, such as an independent body or a wholesale ISP.
- Model 3. The hybrid model, *where the filtering function is managed by a third party, but the customer relations are managed by the ISP.*

There was a slight bias towards the ISP-based model among the respondents to the questionnaire, particularly amongst the larger ISPs surveyed. The hybrid model was the second most popular model, where the third-party filtering provider is a national filtering service that is made available by an approved entity. However, there was little agreement overall on the preferred model, especially among the smaller ISPs.

A major source of disparate opinion amongst ISP's is the opt in/opt out framework. In general, the ISP's have great concern with the potential technical constraints, costs and impact on customer relationships, of applying such a framework.

These results have been interpreted as follows:

- That the option of both an ISP managed implementation as, well as the function of an approved national filtering service, be made available.
- A standard should be set for filtering to ensure uniformity of implementation and practice; and
- Particular attention should be given to the industry concerns with the opt in/opt out framework.

Key Finding 5

There are many important legal and general business aspects that need to be addressed before a decision can be made on a filtering implementation. Frameworks need to be in place to ensure that the legal aspects and responsibility are adequately addressed.

The independent legal expertise that was consulted in developing this report highlighted the following service-specific risks in a mandated filtering scheme:

- Possessing or distributing illegal content;

- Over-blocking and under-blocking content;
- Service degradation and the potential impact on existing service level agreements;
- Interception and hacking;
- Impairing freedom of expression;
- Privacy breaches;
- Contractual claims;
- Negligence;
- Misleading conduct; and
- Breaching sale of goods legislation.

For example, the owner of an inadvertently blocked site might take legal action for damages. Such claims might include actions for:

- Defamation, due to the grave implication that the owner has been involved in the distribution of illegal content.
- Loss of revenue during the time site was blocked, possibly as a result of degradation of product or brand awareness, or direct loss of potential earnings.

Any solution will need to consider compliance and auditing requirements, consistency of implementation, and financial and technical aspects. All of these, in conjunction with the legal aspects mentioned above, would need to be included in any detailed specifications and would require input from content providers, vendors and ISPs.

Key Finding 6

It is evident that there are significant technical problems surrounding dynamic content filtering and its implementation in a nationwide ISP-based content filtering system. Current technology is unlikely to yield efficient and economically viable solutions for this purpose.

Furthermore, the problem is of a nature that requires a research effort before firm conclusions can be drawn on its effectiveness. As the accuracy of this form of filtering is still not high it could be expected that allowed content would be blocked inadvertently. For example, if child pornography is to be blocked, other pornographic content may also be blocked. Conversely, if all pornographic content is to be blocked, other content with a 'resemblance' in features will also be blocked; e.g. sex education, medical information, erotic content etc.

In the opinion of Dr Bjorn Landfeldt from Sydney University, that dynamic content filtering is not a viable option for *mandatory* filtering in its current form. It can only be used in opt-in frameworks because of inherent problems with the accuracy of the filtering. In opt-in frameworks, end users essentially agree to the possibility of some content being incorrectly classified; thereby removing responsibility from any third party provider.

The ISP industry is very negative about solutions using dynamic content filtering. Based on the questionnaire results, the ACMA Blacklist is seen as having the *least* impact on network performance. Dynamic analysis is seen as having the *greatest* impact. Correspondingly, the ISPs do not support dynamic analysis.

Whilst it is evident that ISPs have many concerns over any filtering scheme, the cumulative results suggest that consideration could be given to a national filtering scheme where a URL blacklist of blocked sites is made available to ISPs for filtering.

1.2 Recommended Next Steps

As a result of the findings and comprehensive analysis we recommend the following next steps be given priority:

- Define the objectives of filtering;
- Consider applying the above objectives to a national filtering scheme with particular attention to be given to:
 - The role and scope of a filtering scheme;
 - The implementation options: i.e. ISPs either implementing their own filtering capability or utilising a national filtering service (refer to **Key Finding 4**).
 - The blacklist sources. International sources, such as INHOPE or the Internet Watch Foundation might be considered in conjunction with the ACMA blacklist;
 - The opt in/opt out framework. In particular, consider the implications of making the framework *optional* for ISPs;
 - The implications of making the national filtering scheme *voluntary* for the ISP industry, in line with international precedence.
- Engage with industry to clarify how such a scheme would:
 - Interface with existing ISP infrastructure;
 - Impact on broadband performance;
 - Impact on costs;
 - Handle the issue of recovery of costs to industry as a result of implementation.
- Undertake analysis to determine how vulnerable a national filtering scheme is to circumvention and to attempts to disable it.
- Consult relevant stakeholders regarding the management of the nationwide scheme. Issues to consider include:
 - The legal aspects of such a scheme;
 - Compliance with Australian legislation;
 - Complaint procedures for incorrectly classified content;
 - The scope of filtering (to be undertaken in consultation with the *general public*): what is to be filtered; how often is filtering to be applied; how often will filter lists be updated and provided to ISPs; and
 - How will content be classified; what levels of transparency, scalability and security will apply to the classification process.
- Mobile Internet service providers should be included in the consultation and planning activities.

Undertaking these recommended steps would ensure that a detailed set of requirements could be provided to ISPs. Detailed requirements are necessary for any successful implementation of filtering and for proof of concept testing.

The study has adopted an evidence-based approach and serves as a foundation for a deeper, more informed study. The main issues in ISP level content filtering have been identified and highlighted. The following sections outline the findings of the report in detail.

SECTION A: BACKGROUND AND METHODOLOGY

This section of the report provides *summarised* details on the '*Terms of Reference*' and context of the study. It also provides some information on how the project was conducted.

This information contained in this section is a *summary* only. For the *detailed* information on the background and approach to the study please see Part 2, Appendix B.

1.0 Project Background

The feasibility study on ISP level filtering was initiated in August 2007. The study was supported with funding from the Australian Government through the Department of Broadband, Communications and the Digital Economy (formerly the Department of Communications, Information Technology and the Arts).

2.0 Project Objectives

The objective of the project was to produce a feasibility study into implementation of the ISP filtering component of the national filter scheme, where all ISPs will be required to provide a filtered Internet service for families who *prefer* this protection option.

Without necessarily endorsing the policy of a mandated requirement for ISP level filtering or any particular approach to its implementation, the study is to provide a broad ranging and objective analysis presented by way of a report (in accordance with the following '*Terms of Reference*') on at least three options for the implementation of the Commonwealth's commitment to the provision of ISP filtered services. The analysis includes an examination of technical and performance issues, associated costs, legal issues, the barriers to industry compliance, policy considerations and international precedents.

3.0 Terms of Reference

The following '*Terms of Reference*' applied to the study.

“With regard to the Government's August 2007 policy announcement, but without necessarily endorsing the policy of a mandated requirement for ISP level filtering or any particular approach to its implementation, the IIA will look at the possible scenarios for filtering at the ISP level and quantifies the cost and likely implications of each alternative.

The study is undertaken in consultation with the Department of Broadband, Communications and the Digital Economy (formerly the Department of Communications, Information Technology and the Arts); the Australian Communications and Media Authority (ACMA); ISPs; network/server level filter providers; relevant technology and industry experts; the IT industry; including digital content providers.

The factors that are considered for each scenario include:

- The degree of difficulty in building a system.
- The likely performance impacts on the network.
- The time needed to build the new system.
- The effectiveness of filtering and ease of maintaining current blacklists.
- The effectiveness of and impact on network performance of filtering using URL-based blacklists (e.g. ACMA or vendor-maintained), dynamic analysis, or a combination of both.
- The extent to which filtering would interfere with normal business operations.
- The legal risks to managers of the scheme and the participants.
- The likely build and maintenance costs.
- The degree of end user control and customisation afforded by each approach.
- Ease-of-use for end users, including the degree of transparency.
- The customer support requirements (initial and ongoing).
- Administration costs (initial and ongoing).
- International precedents and the nature and extent of the options employed elsewhere.
- Consistency with existing government policy in other areas; e.g. broadband deployment and uptake.
- Identification of likely barriers to compliance across the whole of the industry.
- The likelihood of disproportionate impacts across the industry.”

The study is designed to complement the ACMA Tasmanian trial. ACMA’s planned trial of content filtering at the ISP level is intended to provide quantitative information about the capabilities of filtering solutions that can be deployed by ISPs. Data produced by the ACMA trial will complement the information this project is supplying on the feasibility and implementation of ISP-level filtering solutions.

It is noted that under the current (new) Governments cyber-safety plan, a filtered internet service will be made available to homes, schools and public internet points accessible by children.

4.0 Limitations

- **Timeframe and Project Scale**

The timeframe allocated for the development and completion of this study was three months (by request). As the majority of ISPs have limited resources (human and financial), their ability to respond to the questionnaire was constrained.

The limited timeframe has also meant that some of the ‘*Terms of Reference*’ – such as ‘Ease-of-use for end users including degree of transparency’ and ‘Degree of end user control and customisation afforded by each approach’ – have not been dealt with in detail. Such terms of reference would require extensive consultation with potential end users. It should be noted, however, that the determination of the implementation models for review has been on the basis that the customer preference for filtering was provided in a way thought to be simplest for the end user.

- **Terms of Reference**

The '*Terms of Reference*' for the study are quite broad and, given the timeframe, the level of detail that the study can provide is limited. Terms of reference such as 'Consistency with existing government policy in other areas ..' were agreed to be dealt with separately from this report.

- **Technical Solutions and Costs**

As part of the '*Terms of Reference*' for the study it was a requirement to provide technical solutions and costs for implementing a solution.

Without detailed business requirements and solution architectures, cost estimates cannot be provided by industry. The variables become too large to provide meaningful data. Technical solutions and costs have been addressed by focusing on implementation issues and comparative costs.

5.0 Approach

The study took place between 9 September 2007 and 3 December 2007. The subsequent report represents an independent and objective analysis based on factual information derived from sources detailed in Part 2, Appendix B subsection 8.2 of this report.

The following methodology was implemented to address the terms of reference.

- Secondary Research
- Primary Research
- Expert Opinion, including:
 - Independent expert technical/industry opinion.
 - Independent legal opinion

The data and information collected from these sources are the foundation of the study. A full list of organisations contacted as part of this study can be found in Part 2, Appendix H of the report.

5.1 Secondary Research

Secondary research was used to:

- 1 Develop a profile of the ISP Industry in Australia
- 2 Gain an understanding of the structure of the content provider industry in Australia
- 3 Extract data from previous Australian studies on content filtering, still applicable to this study.

5.2 Primary Research

The primary research was conducted to provide detailed industry perspectives on:

- The strategic options/management models that could be used to implement ISP level filtering.
- The issues and impacts of ISP level content filtering – particularly those relating to the '*Terms of Reference*'.

Two primary research techniques were utilised:

1. Qualitative data from face-to-face interviews, both in Australia, overseas and from focus groups.
2. Quantitative data from a questionnaire to the ISP industry.

5.3 Expert Opinion

- *Industry/Technology Expert*

An independent industry/technology expert was sourced from the University of Sydney to:

- Provide input into the ISP questionnaire to ensure the statistical relevance.
- Provide an independent review of technical solutions proposed by ISPs or vendors.
- Provide independent technical opinion on the effectiveness of filtering. In particular, filtering using URL-based blacklists and dynamic analysis.

The University of Sydney was selected as it is regarded as one of the leading universities in Australia in information and networking technology.

- *Independent Legal Opinion*

Freehills Solicitors were invited to provide the independent legal opinion for the study. The company provides independent consulting services for a number of telecommunications organisations. As part of this report Freehills were requested to provide advice on the legal risks to managers of each of the management models and of filtering in general.

SECTION B: SECONDARY RESEARCH RESULTS

This section of the report highlights the main findings of the secondary research.

1.0 ISP Industry Profile

1.1 Total Number of Internet Household Subscribers

(ABS: 8153.0 Internet Activity Summary, Australia, March 2007)

- At the end of March 2007, according to the above ABS report, there were 6.43 million active Internet subscribers in Australia, comprised of 761,000 business and government subscribers and 5.67 million household subscribers.

1.2 Size Categorisation of ISPs

(ABS Internet Activity Summary, Australia, B153.0)

Very small ISP	1 - 100 subscribers
Small ISP	101 - 1,000 subscribers
Medium ISP	1,001 - 10,000 subscribers
Large ISP	10,001 - 100,000 subscribers
Very large ISP	100,001 + subscribers

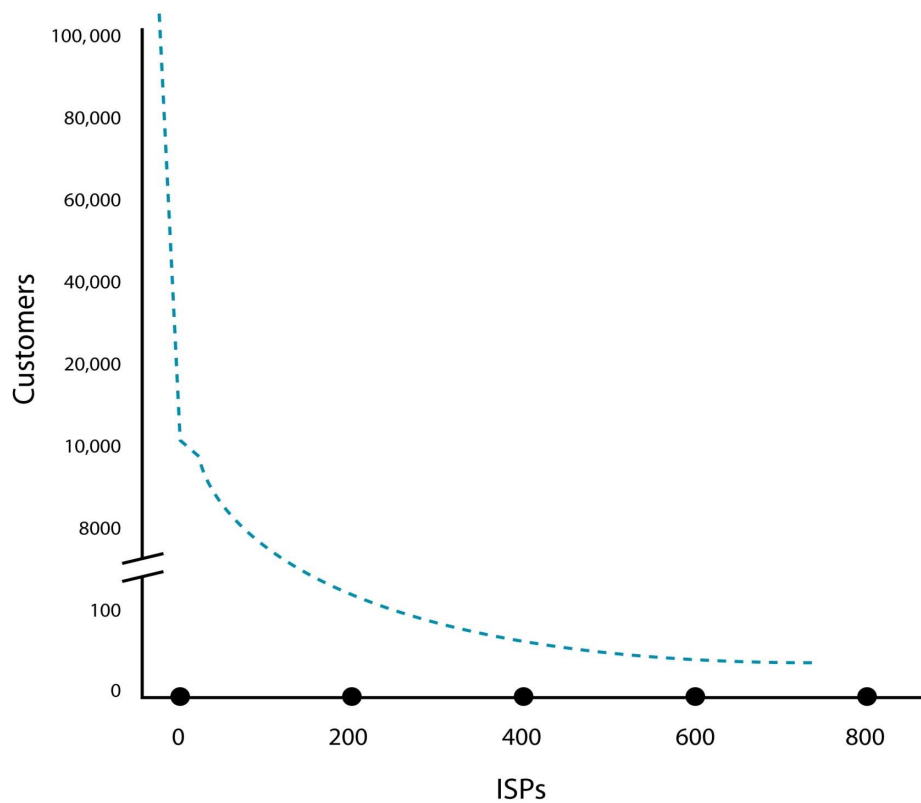
Table 1.0: No. of Large/Very Large ISPs

Category	No. Sept Quarter 2006	March Qtr 2007
Large	22	23
Very Large	10	9
Total	32	32

At the time of writing this report there were approximately 770 ISPs in Australia.

From the data above it can be seen that the industry is dominated by a few key players and has a large number of ISPs with relatively small customer bases: i.e. approximately 738 ISPs in Australia have less than 10,000 subscribers (see Figure 1.0 below). The majority of these 738 ISPs are retailers, of which a large segment re-package or re-sell services provided by other typically large/very large ISPs. In this role these typically large/very large ISPs are known as wholesaler service providers. (see Part 2, Appendix I for supporting data).

Figure 1.0: Profile of ISP Industry by Customer Base



Out of 770 ISPs there are only 32 that have greater than 10,000 customers, 9 with greater than 100,000

This project randomly sampled 323 ISPs from the TIO and IIA lists to extract some high level data about these ISPs. This was necessary because the TIO and IIA lists only provided a URL address of each ISP and no additional data. Thus, it was not possible to ascertain any characteristics beyond the website address details.

Whilst the information is not definitive, from the sample we were able to ascertain the following:

- Approximately 35 ISPs, (or nearly one out of every ten) identified themselves as providing wholesale services. Most do this in conjunction with their own retail services. An example of this would be Optus, which provides wholesale services to a large number of, usually smaller, ISPs but also retails its own OptusNet brand.
- Over one third of all ISPs are based in NSW (see table 2.0 below).
- Approximately 60% of ISPs provide both broadband and dial up services (see table 3.0 below).
- Approximately 70% of ISPs provide national coverage (see table 4.0 below).

Table 2.0: Geographic Distribution

STATE	NUMBER	% OF TOTAL SAMPLE
ACT	7	3.43%
NT	2	
TAS	2	
WA	37	11.5%
NSW	106	33.12%
QLD	38	11.8%
VIC	70	21.8%
SA	14	4.3%
Unknown	42	13.12%

Table 3.0: Technology Type

NO. OF ISPs	TECHNOLOGY	% OF TOTAL SAMPLE
193	Provide both Broadband and Dial Up services.	59.75%
68	Broadband only.	21.05%
8	Dial Up only.	2.47%
51	Did not specify or it was not possible to confirm either via the website or phone.	15.78%

Table 4.0: Coverage

NO. OF ISPs	COVERAGE	% OF TOTAL SAMPLE
217	Provide National coverage (ie: more than one state in Australia).	67.18%
51	Provide either state or regional coverage.	15.78%
52	Did not specify or the data could not be sourced.	16.09%

NB: The percentages in the above tables have been rounded to two decimal places.

2.0 Content Provider Profile

Publishing on the Internet is remarkably easy and inexpensive, and is included as a free service in the end user packages offered by ISPs.

Anyone can be a content producer or publisher. User-generated content is the fastest growing form of content on the Internet:

Over 40 per cent of children and young people have some of their own material on the Internet and a third have a page on a social networking site. Older teenagers are active in Web 2.0. From age 14 onwards, 70 per cent or more of teenagers are engaged in some form of web authorship.¹

For this reason, Internet content providers cannot be conveniently aggregated into an industry sector.

¹ Australian Government, Australian Communications and Media Authority, 'Media and Communications in Australian Families 2007', Report of the Media and Society Research Project, December 2007

However, for the purposes of this study, and based on advice from the AIMIA, it was assumed that the top seven content providers provided over 65% of all content accessed by Australians, including MySpace, YouTube, RSVP, Facebook and adult entertainment. Note that, for the purposes of this study, the Eros Foundation represented the content providers for the 'adult entertainment' industry.

3.0 Related Australian Studies

Over the past decade there have been numerous Australian studies related to Internet content filtering and specifically, filtering performed at the ISP level. These studies have been reviewed and those issues that are related and still relevant to this study have been highlighted.

Details of some of the filtering techniques and methods discussed in this and later sections of the report can be found in Part 2, Appendix K.

3.1 CSIRO, *Blocking Content on the Internet: a Technical Perspective*, 1998

This report recognised two filtering strategies: Internet Packet (IP) filtering and Uniform Resource Locator (URL) filtering, also called 'packet level filtering' and 'application level filtering' respectively.² Both strategies are still relevant and used today. The report noted that IP Filtering was possible without performance impacts if appropriately sized equipment was used.³ It stated that this filtering mechanism could be achieved "*within organisations, at the ISP level, at the Backbone Service Provider level or even at international IP gateways*".⁴

The report noted that IP Filtering, by its nature, is indiscriminate and blocks much more than the content that is being targeted. Filtering, it concluded, "*implemented purely by technological means will be ineffective*"⁵ and that neither IP filtering nor URL filtering "*should be mandated*"⁶. The report added that: "*workarounds will quickly be devised for any technologically-based blocking system.*"⁷ Since the report was produced, workarounds have been well publicised and there are websites and freely available applications dedicated to these and to other circumvention techniques. (Reference: <http://www.peacefire.org/>, <http://www.your-freedom.net/>)

The report made two recommendations on filtering strategies, both of which have been implemented by some Australian businesses.⁸ The first recommendation has been employed by mobile phone companies in the form of a 'clean' service to which access is given to a *permitted* list only (otherwise known as a 'walled garden'). The second recommendation for a 'best effort' service, in which the ISP filters a set of known sites that are rated according to a prescribed criteria (such as a blacklist

² CSIRO 1998 report, page 5

³ Ibid, page 38

⁴ Ibid, page 33

⁵ Ibid, page 39

⁶ & ⁸ Ibid, page 39

⁸ Ibid, pages 39-40

provided by a vendor, or Government blacklist) is utilised by two ISPs for their users: Webshield in South Australia and iTXtreme in Queensland.

The report noted the likely high cost of filtering, recognising that ISPs might not have the capital to invest in the hardware required and that they might not be in a position financially to spend money on ongoing maintenance and training costs for staff maintaining the filtering system.⁹

3.2 CSIRO, Effectiveness of Internet Filtering Software Products, 2001

This report stated that “[a]ll filtering technologies are fallible, and the more the effective they are, the more they risk intruding on general Internet usage”.¹⁰

The report found that:

*Dynamic Analysis [referred to as Content Filtering in the report] ... and detailed techniques employed by different vendors of filtering products ... all of which are less than 100% effective, can result in the inadvertent blocking of useful content, can be computationally intensive and result in an unacceptable slow down in perceived Internet access times.*¹¹

The report noted some additional issues related to the filtering of web content that remain issues in the contemporary climate. For example, in an effort to make web servers more reliable the exact copies of websites are frequently found on more than one server (e.g. www.playboy.com, ww2.playboy.com and ww3.playboy.com). Multiple URLs might be required to handle this situation.¹²

Mention was made in the report that no filtering scheme should expect to be foolproof or 100% effective. Filtering schemes should expect circumvention by a sizeable number of users, even by “those not intending to circumvent it”.

3.3 Ovum Report, Internet Content Filtering, 2003

This report stated that Dynamic Analysis (called ‘pass-through mode analysis filtering’ in the report) had noticeable performance impacts, though it also noted that with increases in processing power “it might become more practical”.¹³

The report also noted that the cost of implementing filtering at the ISP level would be high, and that the sizeable costs involved in the first year's implementation were “unlikely to be regained even if charges are passed on to users”.¹⁴ The costs for ISPs would be ‘initial setup costs [equipment and staff to install and configure] and annual recurring costs [software licenses, support staff]’, while for government, costs would include ‘promotion and enforcement of filtering and maintenance of an authorised

⁹ Ibid, pages, 30 & 38

¹⁰ CSIRO 2001 Report, page 16

¹¹ Ibid, page 10

¹² Ibid pages, 16- 17

¹³ Ovum Report, page 16

¹⁴ Ibid, page 5

blacklist'. The report stated that the impact on small ISPs would be more significant than on larger ISPs, potentially giving larger ISPs a source of competitive advantage, by not passing on costs to users.¹⁵

The report discussed a new technique being employed by filtering vendors, which it called *pass-by analysis filtering*. The technique is typically used for decreasing the amount of time between first access of new content and addition of its URL to the vendor list. The process involves a computer analysis of content in close to real time without holding up the downloading of content. After the analysis the URL, if appropriate, is added to the vendor list for blocking of subsequent access.¹⁶

The report acknowledged that automated (computer-based) analysis of content would produce over-blocking and the extent of over-blocking associated with a blacklist would depend on the processes used to generate it. The report also noted that many vendors, because of inaccuracies in automated analysis, have a process of "*human intervention by which each new URL identified for blocking is checked to identify false positives*".¹⁷ No vendors were identified that offered streaming media or unstreamed moving picture content analysis (i.e. audio or video files and/or streaming) as a part of their filtering products.

3.4 RMIT, A Study on Server Based Internet Filters: Accuracy, Broadband Performance Degradation and some Effects on the User Experience, 2006

This report provided quantitative results on the impact on network performance, including broadband speeds, caused by server-based Internet content filters as well as on the accuracy of such products. It also provided some subjective user feedback on using a broadband service with the filters enabled. The performance results in the report are based on filtering products not necessarily targeted for use within ISPs.

The study revealed that: "*the use of Internet content filters can significantly reduce relative network performance with the level of performance degradation ranging from 18% through to 78%*".¹⁸ The best performing filter that was tested ran at about 80Mbps, much slower than would be required by large ISP networks. Accordingly it was suggested that the speed of filtering would need to be faster than the upstream data connection of the ISP that deploys it, otherwise larger ISPs would need to move their filters further downstream to the edge of their networks in order to filter all traffic.¹⁹

The report concluded that "*while filters can actually perform filtering tasks at relatively high data rates, consideration needs to be given to design, deployment, management, monitoring and redundancy. Cost must also be considered, and would not be small for large deployments.*"²⁰

¹⁵ Ibid, page 57

¹⁶ Ibid, page 19

¹⁷ Ibid, page 17

¹⁸ RMIT Report, page 60

¹⁹ As above

²⁰ Ibid, pages 32-33

SECTION C: PRIMARY RESEARCH RESULTS

This section provides the highlights of the primary research results.

1.0 Management Models For ISP Filtering

The Management Models were defined in initial discussions with the largest ISP organisations in Australia. They were defined based on the requirements that:

- Filtering must be applied
- The customer preference must be also captured: i.e. opting in or opting out.

Once defined, the models were later used as the basis for the face-to-face interviews, the focus groups and the questionnaire.

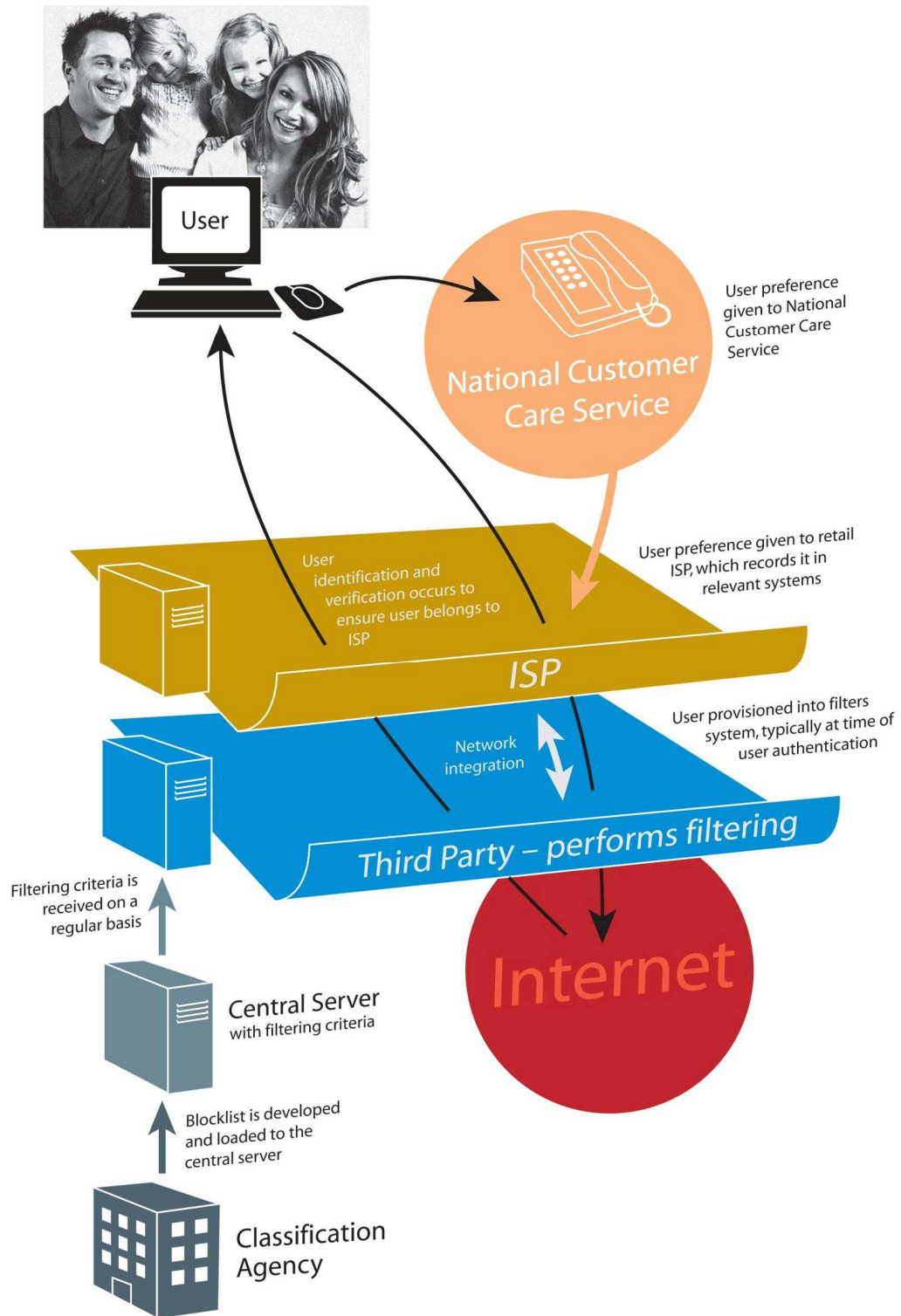
Three management models were identified and defined. These are described in the following pages.

- Option 1 – Third party managed model

This model involves the following components:

- Customers of ISPs make a request to a call centre or website managed by third party to request access to a filtered Internet service. The third party in this model would be a centralised network service.
- The filter capability is externally managed by a third party. There are a number of options as to the third party:
 - A national filtering service provided by an approved entity.
 - Management and operation of the filtering capability by the Wholesale Service Provider; or
 - Management and operation of the filtering capability by a third party provider/vendor approved or accredited by government.

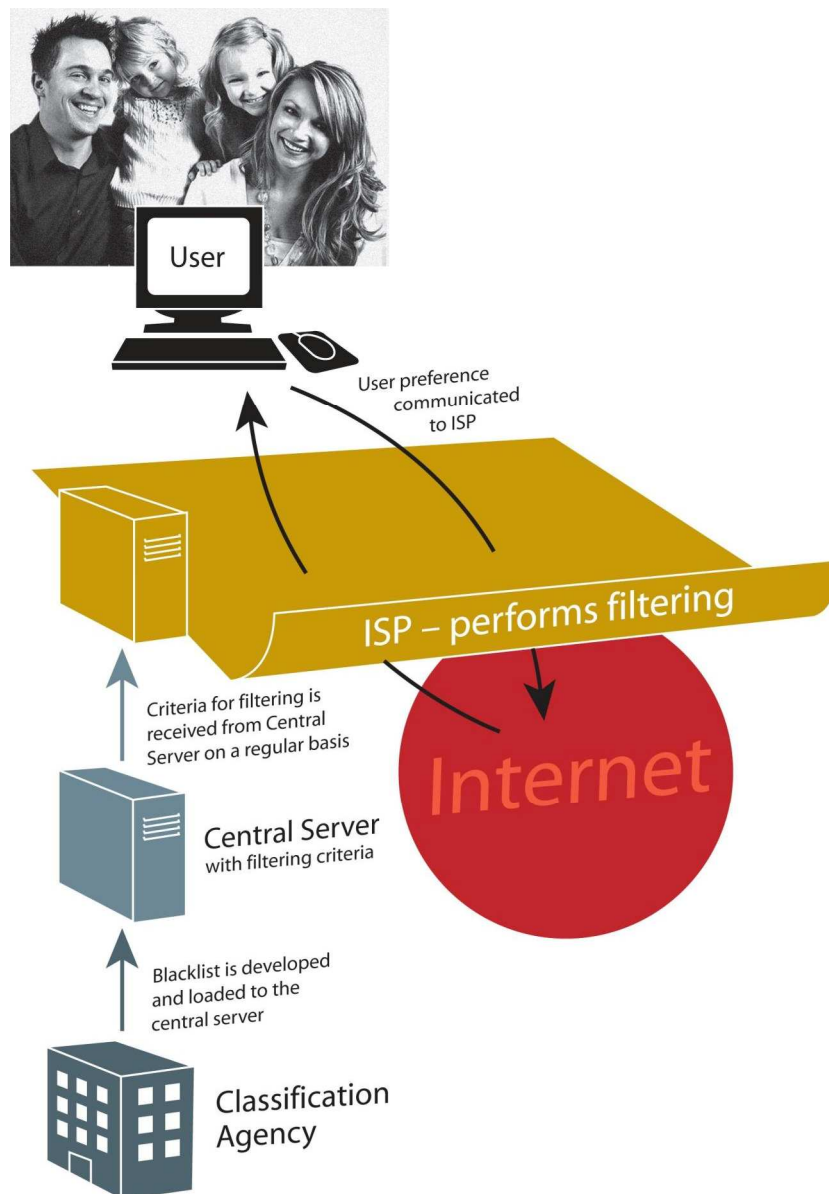
Figure 2.0: Third Party Managed Model



- Option 2 - ISP managed model

In this model the customer relationship is fully managed by the ISP and the content filtering system is also selected, implemented and managed by the ISP. The ISP will need to ensure that any filtering system that is built or selected meets a minimum standard provided by government (for example, that it filters the ACMA black list).

Figure 3.0: ISP Managed Model

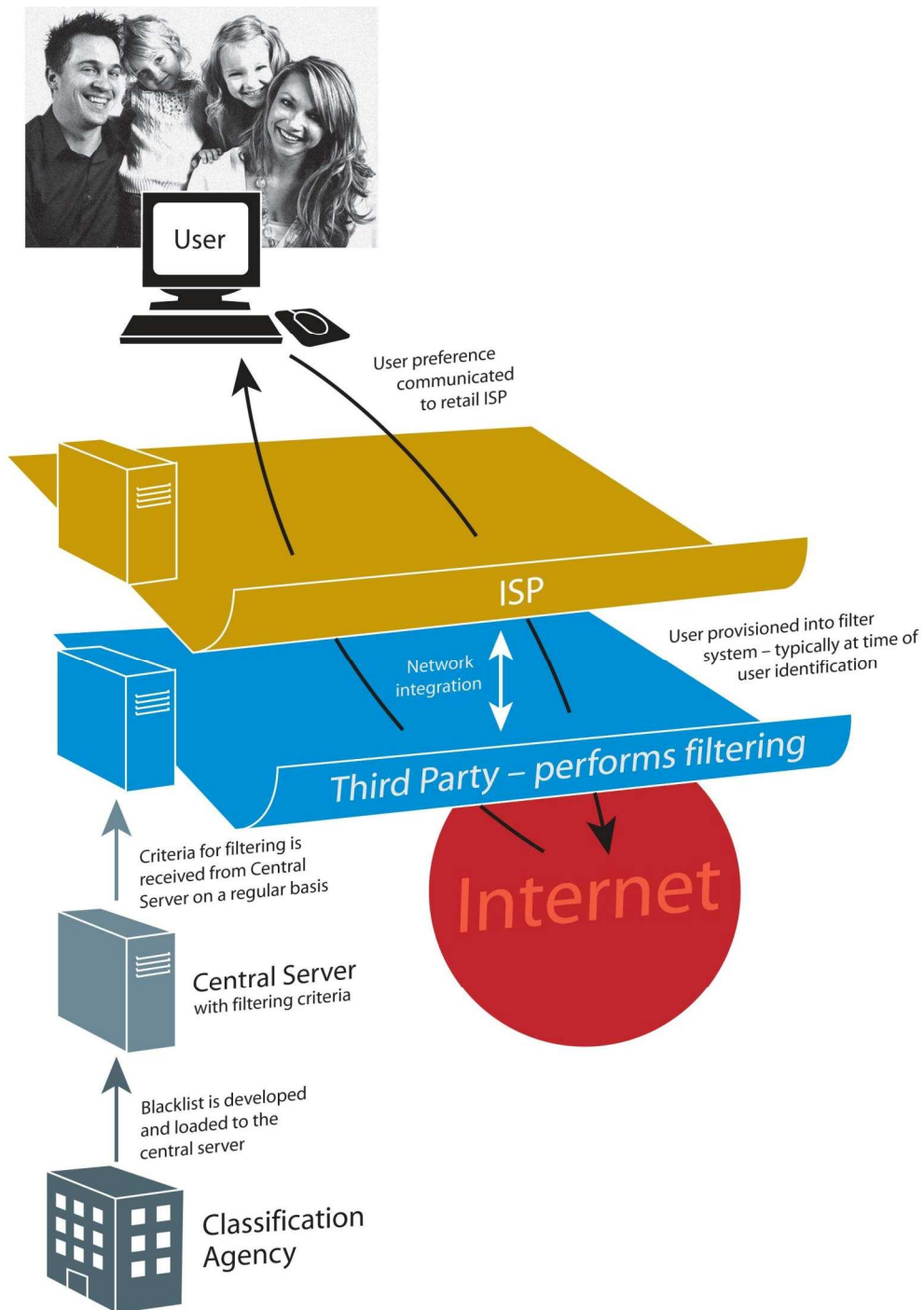


Option 3 - Hybrid managed model

In this model the customer relationship is fully managed by the ISP (as in Option 2). The filter capability is externally managed by a third party (as in Option 3). For example:

- A national filtering service provided by an approved entity.
- Management and operation of the filtering capability by the wholesale service provider; or
- Management and operation of the filtering capability by a third party provider/vendor approved or accredited by government.

Figure 4.0: Hybrid Managed Model



3. Qualitative Data from Face-to-face Interviews and Focus Groups

2.1 ISPs

Twenty-eight ISPs were interviewed or attended focus groups. A range of topics were discussed with the ISPs from the 'Terms of Reference'. Their responses to these topics are detailed below.

- *Management Models*

When discussing the management models during the face-to-face interviews and focus groups, it was clear that the ISP managed model – Option 2 – was *generally* preferred. However, the hybrid management model – Option 3 – also had support.

Many ISPs expressed serious concerns over any management model that included placing externally supplied and managed devices into their network. They felt that doing so would be a major risk to network performance. In particular they felt that speed, reliability and scalability would be outside their control and outside of normal contractual arrangements, especially any service level agreements.

For many of the ISPs a major strength of the ISP managed model was that it enabled them to “*retain the ability to make commercial decisions in implementing a filtering system, as they do with other services they offer*”.

Such decisions would include implementing the solution themselves or contracting their upstream provider to implement it on their behalf. They felt that this would give them greatest control and enable them to insert filtering where most appropriate and in a way that was cost effective. It would also continue to permit them to wholly own and manage their customers and their customers' expectations and be a single point of contact. The hybrid model also had support for these reasons.

At least one ISP stated that they would ask their wholesale ISP for a recommendation on implementation options. This is also consistent with the hybrid model: “*If filtering was mandated, [their] wholesale ISP would most likely be the one to conduct the implementation.*” However, one ISP expressed concern about the competitive and commercial impacts that significantly large wholesalers would have on their resellers. In particular, the ability of resellers to use distributed services for VOIP was of concern, as is illustrated in the following response:

If the major carriers included a filtering solution then they could use [this] government- mandated technology as an excuse for packet delays or disappearing packets etc and thereby kill off any secondary competitive players such as VOIP players. Any packet delay and by definition filtering will delay packets, is detrimental to the competitive landscape. And where would filtering occur - we could easily end up with the same packet getting filtered multiple times on different ISP networks as it moves from one server on one carriers network to another.

The third party managed model caused concern with ISPs because of issues of customer ownership and the willingness to provide customer data to a third party.

Very large ISPs expressed doubts that a third party managed filtering system would be practical because of the enormous quantities of data transiting their networks.

However, one ISP did state that: *“The only model that would be commercially feasible would be filtering of the ACMA blacklist only without user opt-in/opt-out and with a customer service hotline run by the government which handles all customer enquires, complaints, and the like.”*

The more attractive option seemed to be filtering of a single sourced blacklist of URLs, distributed through a completely automated system.

- *Filtering Mechanisms*

Not unexpectedly, most ISPs were not supportive of the concept of filtering, particularly ISP level filtering. Many ISPs highlighted the fact that there are many circumvention techniques. As an example, many stated that VPN traffic and HTTPS traffic would not be able to be filtered.

One ISP felt that filtering was an ‘arms race’, as evidenced by the battle between anti-spam solutions and spammers:

There is an evident risk therefore that web filtering will suffer from the [same] high ongoing costs that email filtering does, as web content providers seek to get their content in front of as many users as possible. For instance, some sites use dynamically generated URLs for each page of content which would make filtering of exact URLs effective only. Such a technique could be employed by such web content providers in order to stymie blacklist filtering.

One very large ISP commented that filtering might not be possible in some circumstances, such as when a user accesses web content hosted on the computer of another user within the same ISP (connected to the same DSLAM or within the same exchange).

The level of support for computer-based filtering techniques (vendor lists, dynamic analysis) was low in general, and particularly low for dynamic analysis. There was a general level of scepticism about its accuracy, as evidenced by the comment made by one ISP: *“How can a computer identify an image from a sweetheart as opposed to some other naked image, both of which might be classified X18+ under current Australian law?”*

In terms of computer-based analysis of content, one ISP stated the following:

Spam filtering is an existing example of filtering using computer based analysis; its record is patchy – there are many false positives and negatives every day. Because of such inherent inaccuracy, a human created blacklist would be preferable and reduce support costs.

Furthermore, regarding dynamic analysis, many ISPs commented that the results of filtering could be inconsistent and thus *“different ISPs would end up filtering different sites”*.

One ISP highlighted the potential for increased design complexity in situations where ISPs employ web caches. Depending on its quality, a web cache might not be able to differentiate web traffic of users who should be filtered (opt-in) from that of users who should not be filtered (opt-out). There's a risk, therefore, that the user who has requested a filtered service sees web content that he or she should not see.

An alternate management model was suggested by a number of ISPs in which filtering is instituted at the international peering level. They suggested that such a model would most likely be the simplest model but would preclude user preference to opt-in or out as filtering would have to be applied for all users.

The alternate management model was seen to hold a number of benefits for those who suggested it, including:

- *“Reducing the number of parties responsible for applying filtering to a very small number.”*
- *“Retail ISPs would not bear the costs and administration costs related to compliance monitoring would be lower.”*
- *“It will promote local content hosting which will come down at full speed (presuming there is a speed impact because of the filtering of internationally hosted content).”*

One ISP expressed general concern about the concept of server-side filtering, stating it was *“a bad idea because server-side filtering technology is not good enough to be rolled out on an ISP-wide model”*. They said that: *“[they] used to run web caching and proxying servers [on which some filtering solutions depend] but stopped when ADSL was rolled out en masse because of the difficulties of scaling to the level needed with the increase in traffic.”*

Existing ISPs offering a filtered Internet service said that uptake by customers is quite high – *“at least 50% of total customers”* – and that there *“is no noticeable performance degradation”*. Whilst only small in number these ISPs all use vendor lists (one uses dynamic analysis as well) and offer more filtering options than filtering off/on. One of the ISPs said that: *“over-blocking has been an issue, not under-blocking.”*

A very large ISP made the point that filtering upstream is not commercially advantageous to them, as *“it will not offer, in terms of ability to leverage mandatory filtering solutions, any advantage to the business and would not permit businesses to personalise their offerings”*. They therefore felt that filtering at the place where the customer is owned is preferable: i.e. PC-based filtering.

At least one ISP said that it would seek to offer a commercial filtering service to its customers and incorporate a mandated blacklist into that offering.

- *Technical and Performance Impacts*

With regards to dynamic analysis the view was unanimous within the industry that network performance would be adversely impacted.

Many felt that the requirement for handling the user preference to opt-in or out of filtering would increase the level of complexity – in terms of technical architecture, business processes and customer support – and accordingly that it would have large cost implications.

It is worthwhile noting that some ISPs suggested that user preference, to opt-in or out, might be difficult in certain situations; for example, in hotels, at free access points, resorts, when sharing net access in buildings, roaming and with prepaid access.

- Cost Impacts

All ISPs felt that dynamic analysis would be very expensive and that any of the costs associated with a mandated ISP level content filtering should be recoverable.

Some ISPs said that they would pass on the costs of filtering to their customers, while others said they would not, and that customers would not pay for a filtered service: *“even \$1/month will be too much.”* In these circumstances they expected that government would cover the costs of mandatory filtering.

A large ISP stated that the imposition of any additional government regulation would make their dial-up service no longer financially viable and they would *“discontinue it as a consequence”*.

There was a general view that offering opt-in functionality would add a lot of additional business overhead and that educating customers on such a system – *“all available options, and what it all means and how it works”* – would be a large and costly endeavour.

Altering business systems to record user preference would be costly for many ISPs, although at least one ISP said that: *“it would not be a big deal because they have many programmers in-house who have developed existing systems.”* In general, the smaller ISPs seemed to feel that they would have the most difficulty in making such system alterations for reasons of cost as well as available resources.

In regard to a filtering scheme in which users must opt-out, the ISPs felt that the costs would be much greater than for a filtering scheme in which users had to expressly opt-in. One ISP suggested that the reason for this was that with *“opting out it would be necessary to scale systems for 100% of users, whereas with the opting in, it was highly likely that only a small percentage of users would select this option thus systems could be scaled accordingly”*. More than the cost of systems, they also felt that with opting in there would be greater staff requirements too.

One very large ISP roughly estimated of the cost of the hardware to examine the protocols of all network traffic (retail and wholesale) as \$2-3 million: *“The cost would certainly be higher if further logic was added to then do something with traffic once it was identified.”*

One ISP was concerned that ISPs would have to bear the cost of complaints to the TIO on matters relating to filtering, as they currently do with other complaints made to the TIO.

- Customer Service

With the exception of one ISP, all ISPs stated that they believed that there would be additional customer support requirements with any form of ISP level filtering. They felt that this cost would be the greatest initially but also would be ongoing. The view most frequently expressed was that customers would always call their ISP with any issue they feel is ISP related. When asked about any differences that may occur with a third party model all ISPs felt that, even if customers were directed to call a third party, users would still call their ISP at some point, if only for an explanation.

- General Issues

Some ISPs expressed concern about the level of auditing required with mandatory ISP filtering, in particular that the level of logging would impact system design and costs.

Regular reference was made to legal intercept as a benchmark for ISP level filtering. This was because such a model mandates that a solution be implemented by an ISP but does not determine which solution and/or which technology is used. Thus the ISP can control the costs.

A number of ISPs suggested that many end users would have little or no awareness of how the ACMA blacklist was created. Many of the ISPs also seemed unaware of the process of developing the list.

ISPs were clear that the government should leave technical decisions to ISPs. One ISP stated that: *“ISPs will need to be able to change the architecture as they see fit, [and] that architecture should not limit commercial flexibility.”*

2.2 Content Providers

Face-to-face interviews were held with nine content providers. The interviews with content providers were focused primarily on the three filtering methods –ACMA blacklist, vendor blacklists and dynamic analysis – and on the concept of ISP level filtering in general and its expected impact.

- Impacts of ISP level Filtering

The following comments relate specifically to adult content.

If users are provided with the option of ‘opting in’ there was seen to be no impact. If opting out was implemented then the impact on the adult content industry was seen to be major: *“Opt-out would add costs and may mean that labelling would be less honest. It would potentially push providers to become more subversive.”*

It was expressed that under mandatory filtering potentially all Australian users of adult content/material would be blocked.

Generally, content providers were concerned that news stories and classified advertising would be filtered inadvertently. One provider commented that they would be *“horrificed if filtering occurred of a legitimate news story on one of [their] sites”*.

It was felt that, initially, filtering systems using computer-based analysis would be likely to have a high rate of false positives. One provider stated their expectation was that *“the algorithms employed would be clever enough to discern legitimate content from prohibited”*.

All of the content providers expressed concerns about filtering using dynamic analysis specifically, and computer-based analysis generally, because of the risk of false positives. They all felt that these filtering techniques could potentially remove valid content from the web. In the words of one content provider: *“Legitimate sites might be blocked accidentally.”* Another provider stated that, with computer based analysis *“access to legitimate educational content, such as biology, anatomy, sexual education would be at risk of filtering.”*

Specific concerns were stated as follows:

- *“Each time filtering parameters are changed [with computer-based analysis], how will the possible impacts of those changes be determined, and who will they get to do it?”*
- *“Another complicating factor with computer-based analysis is human language – what to do with sites not in English?”*

There was a more general support for the concept of filtering using blacklists, specifically blacklists compiled by *“real humans”* and not blacklists created by dynamic search technologies: *“Human generated blacklist is the best way to reduce impact because it has the greatest control over what is blocked.”* One content provider stated that they would *“very likely support filtering based on a blacklist of exact URLs”*. Yet another stated that there would *“likely be only a very low impact on [their] business if ISP level content filtering was introduced based on the current ACMA blacklist rules”*.

Content providers’ concerns about blacklist filtering were noted. In particular the concern that any 'blacklist' should relate to the specific content identified as illegal or harmful, and not to the website hosting that content.

It was felt by all content providers that there was no foolproof filtering solution. This is best expressed in one provider’s comment that: *“Motivated providers of filtered content would change their URLs in order to unblock their pages.”*

- *User-Generated Content*

All the content providers highlighted user-generated content as an area of concern. In the words of one content provider: *“User-generated content [e.g. the weblog] has changed the face of web content publishing on the Internet – and is the future of the web.”* This is further supported by the comment of another provider that *“user-generated content sites are most at risk of inadvertent filtering if an ISP level filtering scheme using computer-based analysis is put in place, because the content is directly published by users.”*

All the content providers predicted a very large increase in user-generated content over the next four years. One provider commented that they were in the process of *“pushing their business in the direction of much more user-generated content”*.

Given the expected growth in user-generated content, the question was raised as to how filtering would be applied in this context. A representative comment in light of this issue was: *“Would owners and/or hosts of filtering content receive notification of such filtering? Without such notification the content owner or host would need to wait till users notified them.”*

- Technical and Performance Issues

For all the content providers, broadband uptake and speed was seen as very important to their businesses. More than one provider expressed concern that filtering would reduce network performance and as a result impact on broadband speeds. This concern is reflected in the comment that: *“Broadband speeds in Australia are low and [they] are concerned about any scheme which degrades existing performance, particularly as it relates to video streaming which has grown dramatically over the past 18 months. Speed degradation would seriously impact that growth.”*

One particular concern expressed by a content provider was that *“any mandatory rules imposed on ISPs must not impose onerous technical obligations or be difficult to implement, otherwise there might be an incentive (or temptation) for ISPs to block entire sites rather than specific content.”*

- Cost Impacts

The discussion of cost impacts focused on inadvertent filtering, specifically:

- Lost revenue caused by a reduced number of page impressions (‘lost traffic’);
- Administrative costs involved in contacting ACMA (or other relevant authority) to unblock sites/pages;
- Costs to the advertiser (e.g. administrative costs, lost sales due to lost advertising, etc.).

With any filtering scheme there is the concern that it might *“get in the way of advertising revenues”*; for instance, if business listings are blocked or the sites belonging to business listings are blocked.

- Customer Service Impacts

Customer service impacts generally focused on the user experience: *“Presenting a user who tries to access blocked content [with] a ‘404 – page not found’ response is not a great customer experience, it would be better to be transparent by offering a message that the content is blocked.”*

Inadvertent filtering was also thought to have an impact on users. It was stated that inadvertent filtering, *“particularly if sites linked to their sites were filtered ... would cause confusion in the user and increase [the need for] support calls to inform them that the link on their site is wrong or to question why they were linking to a site that is prohibited.”*

- General Issues

Content providers expressed the following key issues:

- That the definition of what is prohibited content broadens beyond what may be initially in scope.
- Would filtering be of *illegal* or *undesirable* content?
- That an appeals process was vital to any mandatory filtering scheme.
- Would content be prohibited under Schedule 5 or 7 of the *Broadcasting Services Act (BSA)*? This *“is a critical question because the quantity of content that might be blocked is enormous under Schedule 7.”*

2.3 Filter Vendors

Face-to-face interviews were conducted with seven filter vendors. The primary purpose of the interviews was to discuss their filtering technologies, however the interviews also yielded the following information.

- Management Models

The management models were not discussed in depth with filter vendors, however some of the vendors proposed the following alternate models:

- A filtered government ISP to which customers can move if they want filtering.
- An international gateway model to block international traffic.

It was noted by more than one vendor that existing contracts might not allow inspection of traffic by third parties and that service level agreements would be impacted with any model.

- Filtering Mechanisms

For vendors it was important to know precisely how often a blacklist is updated; how it is distributed; what format it is in; and whether filtering is based on exact or pattern matches.

Vendors generally agreed that dynamic analysis would be far more resource intensive and thus more costly. They also agreed that dynamic analysis with a choice of technologies to implement it would mean different blocking for different ISPs: i.e. inconsistency of filtering across Australia.

Vendors' opinions about filtering were best captured in the following statements:

One vendor stated that: *“When it comes to blocking pornographic content, filtering should be on the domain, not the URL – there are only about 80000 domains from which such content originates.”*

Another vendor stated that: *“The real risk to children is the dynamic content on the Internet, such as instant messages, chat rooms, etc.”*

A very large vendor provided the following comment: *“Get to [a] concrete goal before [establishing] which technology tools could be used to achieve those goals.”*

They went on further to say that: *“If my goal is to stop children from seeing porn, I need to map out two factors: How does the porn industry mass distribute their product today? What approaches are available to bypass barriers to the delivery of their product?”*

All agreed that despite how advanced their technology might be, circumvention was still possible. In the words of one vendor: *“It is difficult to prevent those who have the mind to do so, [from] circumvent[ing] filters.”*

- Technical & Performance Issues

In terms of performance impacts, *“the number of URLs is not the issue; it is rather the act of inspecting traffic in order to obtain the URL that has the performance costs”*.

- General Issues

Nearly all the filter vendors that were interviewed had extensive experience in providing filtering capabilities in corporate environments; some in providing country level filtering capabilities. The following is a list of comments made by various vendors that are of interest when considering filtering and filtering strategies:

- *“Research [should] be conducted with the end user [e.g. parents] on a filtered Internet service and the ramifications of it, e.g. unintended consequences [to the end user] of filtering.”*
- *“The government should mandate standards not technology.”*
- *“There would likely be a large jump in [the] customer support required.”*
- *“The government needs to mandate a minimum level of filtering.”*
- *“In order to achieve national filtering coverage, simplicity and a low level of requirements are key to making it a reality.”*
- *“Access to the blacklist should be restricted,[such] that ISPs would need to agree to levels of protection of the list. Despite that, the list is likely to leak”*

2.3.1 Filter Vendor Technologies

Filtering systems available from vendors are many and varied, offering different functionality, scalability, integration options and more. The selection of one technology over the other is typically predicated on objectives and detailed requirements.

In some instances vendors have added customised filtering for the individual user, rather than adding it just to the ISP customer account. Such functionality usually requires the installation of software on the computer that handles user profile selection and identification, while the filtering is performed by the ISP.

Many vendors also provide technologies that enable filtering to be applied not just to web-based services but also to:

- Email services
- Instant Messaging Services, such as MSN, Yahoo, Internet Relay Chat and Skype
- Peer to peer networks

The above are outside the scope of this study.

2.4 Industry Associations

Face-to-face interviews were conducted with four industry associations. The primary purpose of these interviews was to get a 'representative' opinion.

- Management Models

Comments were received on the different management models. They were general in context and are best illustrated with the following quotes:

- *“With third party and hybrid models, it is likely that the filter provider will be a specialist, which will lead to efficiency and standardisation and consistency across the industry; however the potential for complex integration work is high.”*
- *“With the ISP managed model, there is the ability for ISPs to offer variations on the filtering service to cater for low cost or full featured requirements as required; on the other hand the ISP will most likely not be a filtering specialist.”*

- Filtering Techniques

As with many of the interviews and focus groups, dynamic analysis was seen to be problematic: *“If content filtering is conducted on the basis of dynamic analysis [i.e. computer based determination of the category of content], then mis-categorisation or over-blocking would occur across the board. For example: ‘nude shoes’, ‘breast cancer awareness programs’ etc”.*

During one interview it was pointed out that content acceptable in some broadcast media (i.e. radio or television), when on the Internet, would be at risk of being blocked by dynamic analysis.

It was also flagged that the government is one of the largest publishers of digital content in Australia, with the comment being made that: *“programs such as rape counselling and more... would be at risk of being incorrectly categorised through dynamic analysis.”*

- General Issues

It was pointed out that any form of filtering would be fallible. *“Many people will work to find ways to bypass the system for academic interest, freedom of speech, making a political statement, etc.”* Specific examples of circumvention techniques were provided.

- “Users will use VPNs and similar tunnels to evade a system.”
- “Networks such as The Onion Router (TOR) exist to [make] traffic [anonymous]. They are simple to use and will be heavily used.”

It was suggested that a blocked page should report to the user what category the page visited belongs to, and why it is blocked. It was felt that this would “*allow the user to choose to call in to report a mis-categorised site.*”

2.5 International ISPs and Overseas Regulatory Bodies

Face-to-face interviews were held with 20 international ISPs (including seven national ISP representative organisations) and four overseas regulatory bodies, amongst others (see Part 2, Appendix H). The interviews were conducted in September and October 2007. The following information is the result of these interviews. More detailed information can be found in Parts 3 & 4 of this report.

- Technical Assessment

Of those countries and overseas regulatory bodies visited:

- ISP level filtering is more commonly performed in Europe. ISP level filtering is not currently performed in the USA (at the time of the study).
- Both Domain Name System (DNS) filtering and URL filtering are used. There appears to be no clear preference.
- In some countries there are no agreed upon methods of implementation.
- A majority of them source the list of URLs (sites) to be filtered from law enforcement; and some from government departments, Non Government Organisations (NGOs) and other sources.
- A majority have opted to serve up a 'blocked' page. In the UK a user receives a '404, page not found' error message.
- Child pornography is primarily filtered, although one country also filters gambling.
- In some countries not all of the ISPs offer filtering; in some cases ISPs with subscriber numbers below a minimum base level are exempt from having to filter or offer filtering.
- In at least one country there is a distinction made between the possession of commercial and non-commercial child abuse images.
- Some countries seek to distinguish between illegal sites and restricted sites, the access to which could be limited by age verification.
- In some countries legislation provides immunity for ISPs against liability for being a 'mere conduit' between user and content host.
- The ISP industry, in at least one country, is pursuing filtering solutions that provide more granular control to individual users (i.e. the ability to personalise their filtering), as opposed to a one size fits all solutions.

- Regulatory Frameworks
 - Some overseas countries have constitutionally protected free speech “*which creates limitations on the extent of content filtered, specifically on the range of content which can be filtered*”.
 - European Community parliamentary legislation currently provides that: “*Internet Service Providers are not liable for content on their servers or network infrastructure put there by third parties unless they fail to remove content once they have been informed about its illegality [e.g. through a hotline].*”
 - With regard to the success of filtering web content, the Finnish Ministry of Communication “*agrees that the system can not prevent all intentional access to child pornography. Most child pornography is not distributed through web pages with static IP addresses, but rather through alternative mechanisms such as newsgroups. IP-based censorship is also easily circumvented using any of the numerous free proxy services available on the web.*” Finland accepts that “*the system will not stop most persons who intentionally attempt to access child pornography pages.*” The additional point is made that: “*the system will prevent Internet users from accidentally accessing pages that contain child pornography.*”
 - Concerns have been raised overseas in regard to the lack of transparency that is offered, particularly in the approach of not displaying a ‘blocked’ page but rather making the requested web content non-existent (i.e. through a ‘404 – page not found’ error message).
 - Concerns have also been raised overseas in regard to publicly accountable procedures. This concern is illustrated by the following example from Denmark: “*An innocent site was blocked and the owner challenged the ISP. The ISP argued he was given the list by the police. The police said they only recommended the sites.*”
 - Noteworthy is the fact that, in the European Union, compliance with filtering remains voluntary, with the exception of Italy in relation to gambling sites. “*Compliance by industry, which is at best patchy, is nevertheless predicated on the assumption that it is only child abuse images which will be blocked.*”
 - Whether the objectives of ISP level filtering are being achieved is uncertain. In Sweden those involved have acknowledged “*that the scheme is not 100% effective*” as a result of factors such as the size of the list; that sites identified are not taken down because they are usually outside of the country’s jurisdiction; and access to identified sites is still possible via proxy or other mechanisms. For these reasons, effectiveness at large is difficult to judge.

More detail on the international regulatory frameworks and environments is contained within Part 3 of this report.

3.0 Quantitative Data from Questionnaire

This is a high level summary of the key results only. The detailed report can be found in Part 2, Appendix F.

3.1 Questionnaire Results

A total of 34 completed questionnaires were received. This represents:

- 4.5% of the total number of ISPs in Australia
- 10.6% of the profiled ISP list
- 53% of the total number of questionnaires distributed.

This number is sufficiently large to consider the dataset to be representative of the retail ISP industry in Australia.

All wholesale service providers who took part in the survey also identified themselves as retail ISPs.

3.1.1 Retail ISP Responses

In general, the ISP managed model was the preferred model, with 53% (or 18) of respondents selecting it. However, the hybrid model was a close second, with 32% (or 11) respondents preferring this model.

All of the ISPs with less than 1000 customers preferred the third party model. When combined, the third party model and hybrid management models almost equal the ISP management model in terms of preference, with 47%.

The results suggest that the industry is divided. It is clear from this that the government would still be required to give options to ISPs on the management model to be implemented. No one method should be presented to industry.

For those ISPs that selected the third party or hybrid management models the questionnaire asked what type of third party filtering service they would prefer. Sixty-three percent said that they would prefer a national filtering service.

When asked to rank a number of potential reasons for selecting their preferred model, 44% of respondents ranked '*We retain ownership of the customer*' as number 1 and 15% ranked '*It enables us to manage the customer experience*' as number 2. Among the reasons for not selecting another model, the two reasons '*We do not retail ownership of the customer*' and '*It does not enable us to manage the customer experience*' made up 68% of the responses.

From this we can conclude that the main concern for the ISPs surveyed, when the preferred model is considered, is the relationship with their customers.

When asked about the level of difficulty in implementing a system, the following results were obtained:

- In general, all ISPs expected any implementation of filtering to be difficult and to have impacts on their existing infrastructure. This includes design impacts on existing infrastructure, when integrating with a content filtering system or, in the case of the third party mode, on a third party customer care service, and also includes deployment impacts with existing infrastructure.
- The results suggest that any implementation will impact the most on smaller players as a result of resource constraints.
- When asked how long it would take to implement a filtering system, regardless of the model, the majority of the industry believed that it would take up to a year to implement.
- In terms of costs, the ISP managed model was seen as having the highest build and maintenance costs.
- When questioned about filtering it was evident that dynamic analysis was deemed to have the greatest costs, the largest network design and IT systems impact, and impact on network performance.

Conversely, dynamic analysis was the filtering mechanism least supported by the ISPs. Comparatively, the ACMA blacklist had the greatest level of support.

3.1.2 Wholesale Service Provider Responses

Fourteen respondents to the questionnaire described themselves as wholesalers. It is important to recall here that it is possible to be both a wholesale service provider and a retail ISP. Because of the small number of wholesalers represented in the survey and in the industry as a whole, the results are aggregated rather than cross-tabulated. Cross-tabulation is only possible with a larger sample size.

Out of the respondents one selected the third party managed model, two selected the hybrid model and nine selected the ISP managed model. Out of the third party and hybrid models there was no consensus on the reason for selection. The respondents who indicated the third party management model were neutral regarding any difficulty in designing and deploying the system.

Most commonly, as wholesalers, the respondents saw themselves as being the ones who would ultimately apply any filtering solution. With the exception of one wholesaler, they all thought that the implementation of a filtering system was difficult, typically because of the additional support and contractual arrangements required. An open-ended response provided the following reason for this belief: *“Any filtering solution will incur a support overhead which will inevitably come to us as the primary service provider.”*

**SECTION D - FILTERING IMPLEMENTATIONS, AUSTRALIA
AND OVERSEAS**

1.0 Filtering Implementations

ISP based filtering implementations are predominately based in Europe. The information below summarises the filtering implementations found overseas. For a full report see Part 3 of this report.

1.1 International Implementations

1.1.1 Denmark

In Denmark currently, child abuse images are the primary focus of filtering. Filtering is performed at the ISP end, although participation is voluntary and does not span the entire industry. The filter lists are maintained by the police.

In terms of market share, the main players are TDC, Telia and Cybercity, which collectively cover about 90% of the market. The rest of the industry is comprised of many smaller players who are not filtering. This is consistent with the approach taken in the Danish anti-terrorist legislation introduced in 2004 and 2007. These laws require the logging of all traffic, but expressly exempt ISPs with subscriber numbers under about 100-200.

ISPs implement internally as they see fit. Filtering occurs at the DNS level, not at the IP Level.

1.1.2 Finland

In Finland, a voluntary program has been implemented by ISPs to curb access to foreign web pages containing child pornography. This has been in place since September 2005. There is no legal obligation for ISPs to block sites

In practice, ISPs prevent access to a list of IP addresses supplied by the Finnish police. The list is maintained by the police and based on web pages suspected to contain child pornography. The list is not publicly available.

1.1.3 Germany

There is currently no mandatory requirement to filter Internet traffic in Germany. However, on a case-by-case basis, ISPs may be required to limit access to sites at the direction of a court or other public authority.

Most German ISPs implement filtering using DNS poisoning. In Germany, the industry and government seek to distinguish between illegal sites and those that would be restricted (e.g. adult sites), which could be limited by age verification.

The German industry is pursuing user autonomous solutions (i.e. end user options), as they give more granular control. The regulator - KJM - has chosen not to tackle ISPs on filtering, so the current scheme is not enforced at large.

1.1.4 Ireland

Irish ISPs must act in reasonable time to remove illegal content from public access on systems under their control of which they have been given knowledge. ISPs are only expected to act in a reactive mode and can only act to suspend accounts or remove content hosted on systems directly under their control in their jurisdiction.

The industry has largely been given the right to self-regulate in the area of child protection generally.

1.1.5 Italy

In Italy, since 6th February 2006, ISPs have been required to have processes in place to deal with access to child pornography. Specifically, there are “filtering mechanisms to prevent access to proscribed sites as advised by a special centre dealing with such activities”.

No direction has been given as to technical implementation. Only ISPs who provide connectivity to the Internet to consumers (not to other ISPs) have to comply with this decree. ISPs must implement filtering of the sites on the blacklist *at least* at fully qualified domain name level (FQDN) or, if expressly requested by the police, at IP address level. In the Italian context, filtering means forwarding the web request to a specific web page created by the ISP, the contents of which page are determined by the police.

1.1.6 Norway

In Norway, filtering remains a voluntary system and there is no sanction for non-compliance. Each ISP determines how they wish to block access. ISPs can implement filtering as they see fit. Based on interviews, it is understood that DNS filtering is the preferred option amongst ISPs.

1.1.7 Sweden

In Sweden, the system of blocking is presently voluntary and is implemented by self-regulation within the industry.

The content that is blocked is expressly confined to *commercial* child pornography sites: i.e. sites that offer child abuse images for sale.

In Sweden, all major ISPs are participating in these voluntary arrangements.

The method by which notified sites are blocked is left up to each ISP to determine. Typically, this is done at the DNS-level, whereby caching-servers are configured to catch all queries to sites listed by the police.

When a user requests access via their browser to a blacklisted site, their browser request is replied to with a fixed IP address, namely the police ‘STOP’ site. This

presents a page that explains why access to the page has been blocked and refers questions to the police.

There are four main underlying purposes to the scheme:

- To stop accidental access (protect customers)
- To restrain recruitment of new consumers of illegal images
- To assist in preventing the sexual exploitation of children
- To remove any financial incentive to produce child abuse images.

1.1.8 United Kingdom

British Telecom (BT) introduced Cleanfeed in June 2004.

In the UK, ISPs are at liberty to choose the method by which they remove the content – some are using the BT Cleanfeed technology, while others are resorting to simple DNS blocking.

The object of the filtering is “to stop casual voyeurism, accidental access and search engines”. System design occurred with that objective in mind, and with the understanding that any circumvention techniques available – and employed by those with a mind to do so – would not prevent the objective from being achieved.

BT has around 5 million retail customers, and since filtering has been enabled for BT’s entire network, close to 20 million users – both wholesale and retail – are now being serviced. The customer base is predominantly broadband. BT has stated that the Cleanfeed system has had no impact on network performance. They have stated however, that the system has only been designed to handle a limited number of sites confined to the Internet Watch Foundation (IWF) list of URLs used in their filtering process.

1.1.9 Canada

In Canada, ISP filtering is voluntary. Lists are provided by www.Cybertip.ca, which creates and maintains “a regularly updated list of specific foreign-hosted Internet addresses [URLs] associated with images of child sexual abuse and will provide that list in a secure manner to participating ISPs”.

Participating Canadian ISPs implement filtering to automatically prevent access to addresses on the list.

The adding of a new URL to the list is via a complaints-based process, which is similar to the current ACMA process. Review of URLs on the list occurs on a weekly basis through the use of automated systems that flag any URLs that have had content changes, and analysts review those that are flagged.

When blocking occurs, there is no indication that it has been applied. Users are presented with a standard 'page not found' error.

It is at the discretion of each ISP to decide whether they wish to participate in the Cleanfeed Canada program.

The focus is only on content hosted outside Canada and on child pornography.

Note: This information was sourced from http://www.cybertip.ca/en/cybertip/cf_faq
As such it is not included in Part 3 of this report.

2.0 Australian Implementations

Two Australian implementations of ISP level filtering were identified during the study period. The companies are Webshield and ItXtreme Pty Ltd. Both these organisations were developed with the explicit purpose of offering ISP level content filtering services under contractual arrangement to their customers. Webshield has offered these services from the time of establishment, and ItXtreme since shortly after establishment.

The following material was provided by each organisation.

2.1 Webshield

Webshield was founded in February 2004, providing dial-up Internet services. Webshield now supplies dial-up, ADSL 1 and hosting services, with ADSL 2 services being planned for the near future.

- *Why offer content filtering?*

The founder investigated PC-based filtering solutions but quickly found that the skill required to maintain the filters put them out of the technical reach of many families.

Focus groups indicated that there was value to be found in a service that removed the need for the family to be 'up to speed' with current technologies and made the Internet a safer place with which to interact.

The design standard set for filtering technology was "to stop an addicted user from locating inappropriate material in a premeditated search".

The three main components to the Webshield content filtering technology are detailed below:

- 1) The URL content Filter
- 2) Layer 7 packet filter
- 3) The port filter

- *The URL Content Filter*

When deciding on a content filter, there were a number of options available. The three key decision criteria were:

- Categorisation accuracy – categories needed to be accurate in their classification and updated at least daily to match the dynamic nature of the Internet

- Speed – the filtering device needed to be capable of making a block or pass decision without adding noticeable delay to the customer surfing experience.
- Scalability – the product needed to be capable of starting out small and growing as the business grew.

The content filtering device selected is a US product and specialises in filtering Internet sites at a URL and IP address level. The content filter is based on vendor-categorised lists and boasts the largest and most accurately categorised database of sites in the world.

Features include:

- Over 94 different categories
 - Blacklist and ‘white’ list filtering
 - Block peer-to-peer, bit torrent and chat
 - Search word and key word filtering
 - Lock in Google/Yahoo family filter
 - ‘X’ strikes filtering
 - Timed filter profile
 - Configurable block page
- Layer 7 packet filter

The Layer 7 packet filter interrogates the data stream as it passes through the network. Its role is to identify and classify traffic allowing for more granular pass or block decision making that a content filter by itself is not capable of recognizing.

The Layer 7 filter is programmed to recognise over 100 different web-based protocols and is scalable from 20Mbps of traffic throughput to over 4Gbps.

In addition to providing protection for Internet protocols, this technology has the capability to closely manage Internet resource usage, saving up to 30% on bandwidth costs.

Features include:

- Protocol Filtering
 - Bandwidth optimisation
 - Bandwidth analysis
 - Bandwidth prioritisation
- The Port Filter

The third element in the filtering solution is Webshield’s own custom designed port filtering technology, which is designed to act in the same way as an intelligent firewall.

Traffic passing through various firewall ports is interrogated by the port filter, opening and closing ports as required ensuring an even higher level of filtering protection.

The port filter monitors traffic via these ports and can block or pass any combination of ports on a per user basis. This added level of protection:

- Prevents the bypassing of filtering through a proxy port.
- Prevents common P2P transmission ports.
- Can be used as an additional block for chat protocols.

2.2 ItXtreme

ItXtreme Pty Ltd was founded in Rockhampton, Queensland in 2002 and offers a nationwide ISP service. It is a separate business operating under Queensland IT Solutions Pty Ltd.

In 2003, the company decided to offer content filtering as part of its service. Negotiations were conducted with a company who provided corporate content filtering and a method of adapting this product for home use was developed. The resultant product is ISP server-based.

ItXtreme enable or disable the filtering at the request of the customer. The ItXtreme system is updated every hour, so that recent 'problem sites' are blocked very quickly. The filtering mechanisms deployed include both dynamic analysis and blacklists.

SECTION E - TECHNICAL ASSESSMENTS

This section contains:

1. Information on the processes for classifying content, particularly as they apply to filtering of the ACMA blacklist, vendor-maintained blacklists, and/or dynamic analysis. It is based on information collected during the study process.
2. Independent technical assessments of:
 - a. Category based filtering
 - b. Dynamic analysis.

The independent technical assessments were provided by Dr Bjorn Landfeldt from Sydney University.

1.0 *Filtering Classification Methods*

The vendors interviewed for this study generally used two main methods for classifying content:

- *Human*-based classification
- *Computer*-based classification.

Both methods involve the establishment of criteria against which content is tested and then classified.

Human-based classification: Typically, a human-based classification process involves detailed manual processing of content and data. It usually requires some time for completion but can result in more accurate classification of content being achieved.

Computer-based classification: This involves the use of automated systems applying specific criteria to content. It can be done in real time or in a few minutes. The time to complete the classification is influenced by factors such as the complexity of the criteria to be applied and the power of the system performing it. It is typically less accurate than human-based classification.

More detail is available on the types of computer-based classification techniques (see Ovum Report, *Internet Content Filtering*, 2003, pp.19-20). The types of processes implemented, after the content is classified, are discussed in Section E, Subsection 2.0 (*Independent Technical Assessment*) of this report.

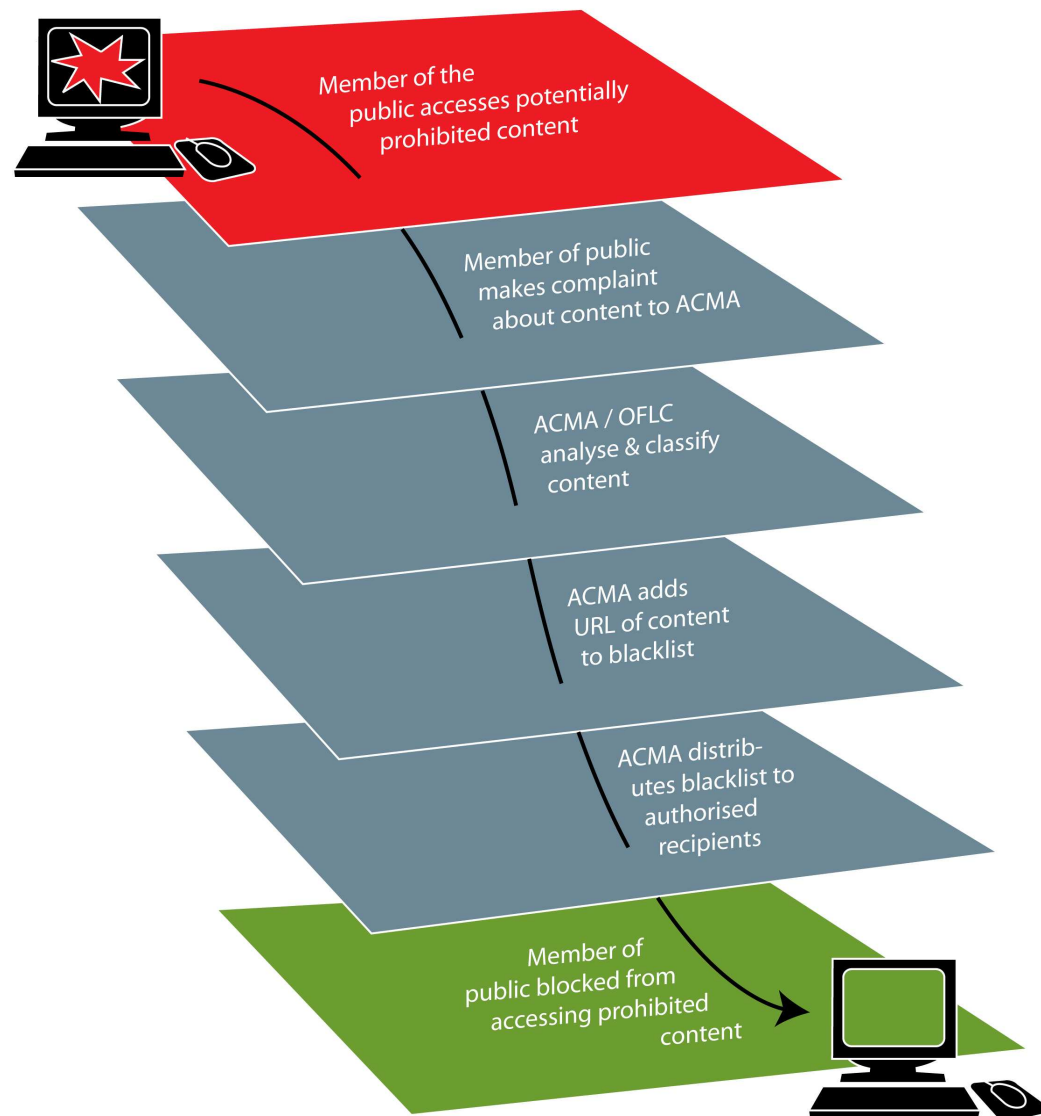
1.1 ACMA blacklist

Australia already has a list of *prohibited* online content as defined by the Australian Communications and Media Authority (ACMA). This list (also referred to as the 'ACMA blacklist') contains the URLs of content prohibited in Australia. The classification process is human-based and is usually initiated through a complaint from a member of the public. The ACMA blacklist contains exact URLs.

See Part 2, Appendix L, for detailed information on the ACMA blacklist. See overview diagram, Figure 5.0 below.

Figure 5: ACMA Blacklist Classification Process

Overview – ACMA Blacklist Classification Process



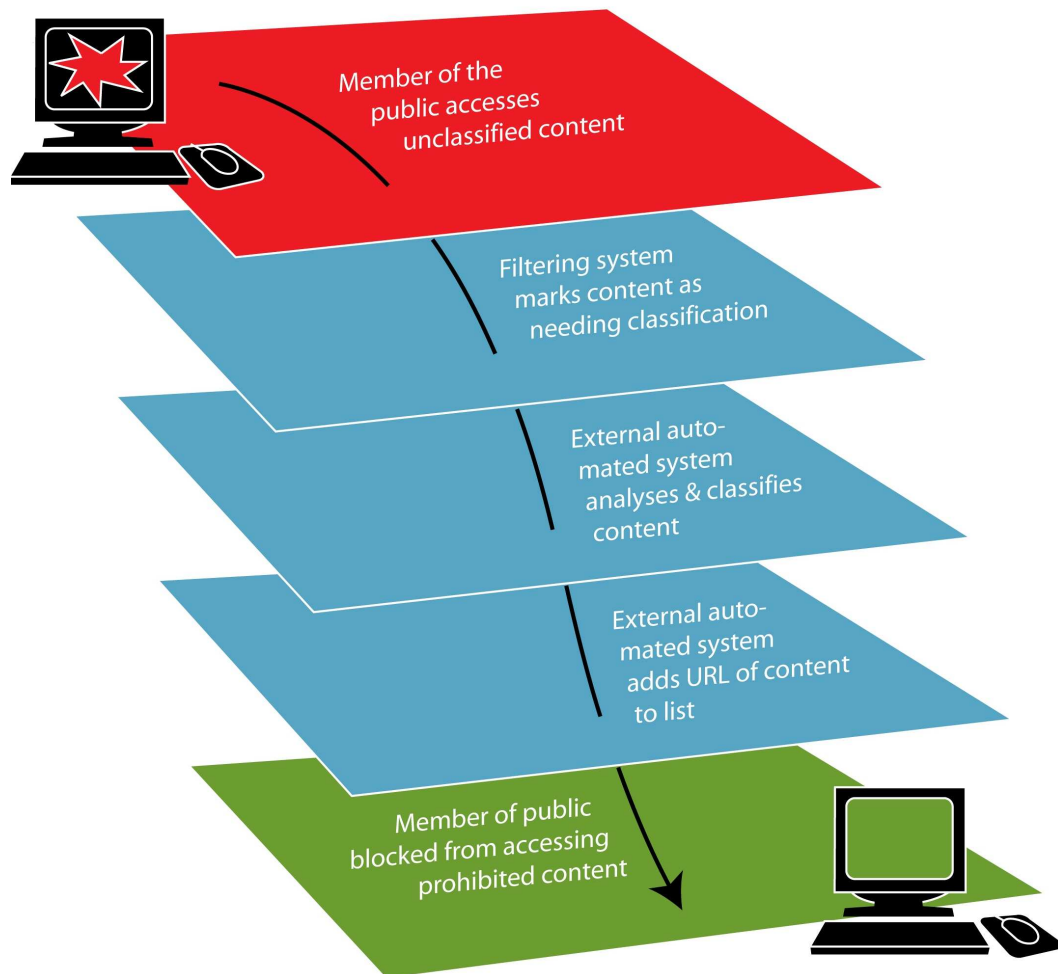
1.2 Vendor-maintained blacklists

Typically, vendor organisations such as those interviewed during the study process, use a combination of both human classification and computer classification. Additionally, they will often utilise blacklists that have been compiled by a number of organisations, such as ACMA and the Internet Watch Foundation (IWF) in the UK.

Filter vendors will frequently use these blacklists, often in combination with other filtering techniques (described in Part 2, Appendix K), in order to block access to that content. Some filter vendors provide services that enable content filtering to be personalised to meet the end user requirements.

See diagram – Figure 6.0 below.

Figure 6: Vendor Blacklist Classification Process



1.3 Dynamic Analysis

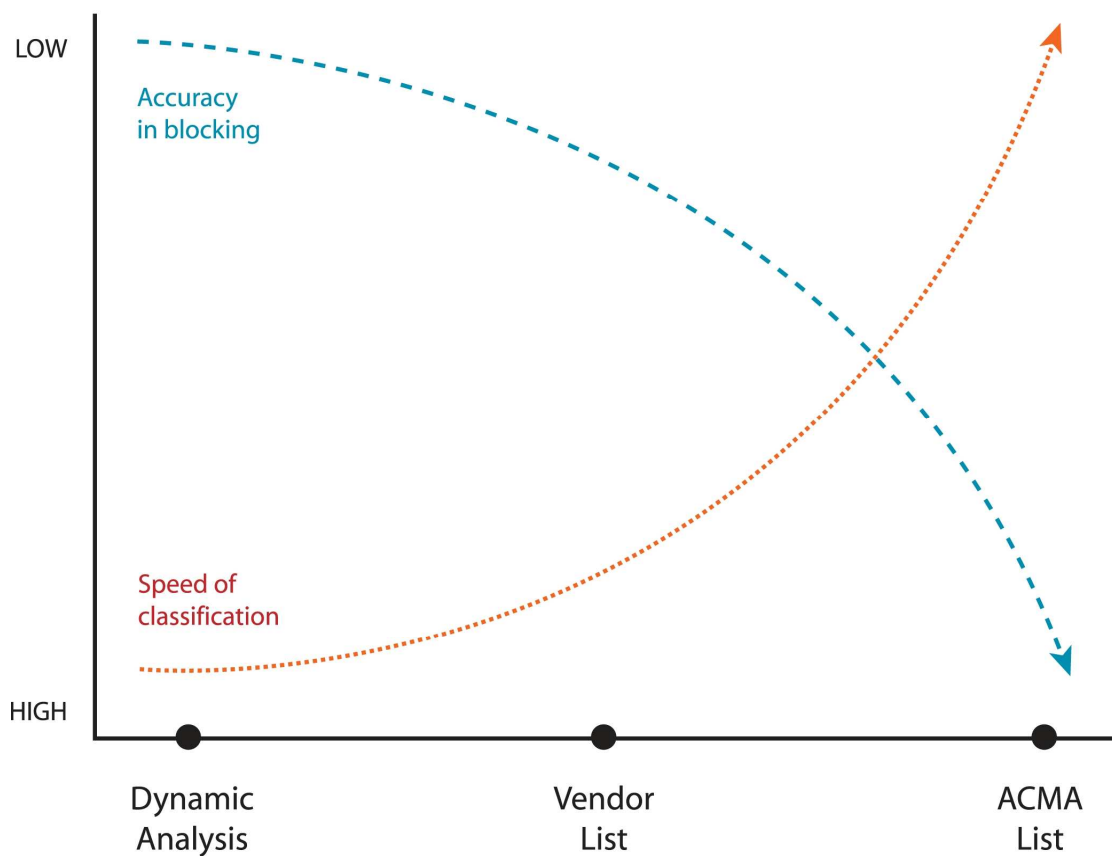
An alternative to filtering based on an ACMA or vendor blacklist is dynamic analysis. This is filtering based on analysis of the content as it is being downloaded. Because it is in *real time*, content classification is *computer*-based, and can therefore have a bigger impact on end users' computer speeds (see Part 2, Appendix K and Subsection 3.0 below for detailed information on dynamic analysis. See also the RMIT study, *Server Based Internet Filters*, 2006, Section B, Subsection 3.4).

1.4 Strategic Implications

Regardless of the filtering classification method used i.e. human or computer based; content classification accuracy “*is linked to how much resource the analysis process requires and how long it takes to perform*” (Reference: Ovum Report, *Internet Content Filtering*, 2003, pp 24-25).

The evidence suggests that there is a trade-off between classification ‘accuracy’ and ‘speed’. This may need to be considered when determining the objectives of a filtering scheme. See Figure 7 below.

Figure 7 - Classification Speed vs Accuracy - ACMA Blacklists, Vendors Blacklists, Dynamic Analysis



This subsection of the main report contains summaries of the independent technical assessment. The complete assessments can be found in Part 2, Appendix M, of this report.

2.0 Category-Based Filtering

The information below provides further detail on the technical processes underpinning content classification and their associated risks and constraints.

2.1 System Aspects of Content Filtering

The Internet industry has reached a stage where filtering and classification is common practice for many purposes.

Content filtering is currently done on most end-nodes attached to the Internet in the form of firewalling, blocking of components such as cookies and active code modules, filtering for viruses and Spam and offensive web page content. In many production networks, Layer 7 switching is done to optimise application performance or to penalise applications such as peer-to-peer traffic.

However, such systems need to be defined and implemented with great care, as the issues surrounding content filtering are often complex, and poorly engineered solutions can lead to performance degradation and increased costs. The following articulates some of the issues surrounding content filtering.

2.1.1 Importance of Aims and Policy

It is impossible to form a firm opinion on the suitability of technical solutions and organisational impacts without a clear understanding of the aims, goals and scope of the system. For example, for an ISP-based system it is necessary to define if the system is meant to prevent prohibited content occurring on the Internet, or if it is meant to completely block or minimise the risk of inadvertent access.

‘Prohibited’ and ‘classified’ content are dealt with in more detail below.

2.1.2 Technical Considerations of Content Classification

Determining if content is in breach of Australian law has to be done by an authority with legal expertise and a mandate to make the determination. Such content also requires policing and possible further legal action, as well as interaction with international bodies. It is therefore natural that the classification is managed by a central authority with a mandate from government.

The sensitivity of the data creates the necessity for the tight control of both distribution and management. If the content classification is made public an offender has a significant advantage, in that it is typically easy to move content to a different identifier (URL), whereas the process of locating and blocking the content is onerous by comparison.

It should be noted that the amount of content generated on the Internet is enormous and that it is an onerous task to scan the Internet for possible prohibited content. For

example, video can be encoded at different data rates, ranging from tens of kilobit per second to several megabit per second. This translates to file sizes between the order of 10 megabyte and 10 gigabyte per hour of video content. Given the large file sizes for video this translates to significant bandwidth requirements to download the media for analysis. It is therefore not practical for an Australian authority to scan the Internet for prohibited media through off-line processing.

It should also be mentioned that blocking of prohibited content is typically not implemented in an opt-in/opt-out scenario. Implementing systems for blocking such content have therefore had little or no impact on customer relations and management.

In order to categorise content through computer-based classification, it is necessary to adopt some form of dynamic content analysis, as the sheer volume of data in this category exceeds what can be managed manually. (Dynamic content filtering is dealt within more detail in Subsection 3.0 below)

There are a number of filtering systems commercially available for this purpose, including end user system (PC) filters. The end-user filters are implemented through an opt-in mechanism and, therefore, any implications following wrongful classification are removed from third parties.

There are also a number of commercial systems implemented at the ISP level. These systems provide the same basic functionality as the end-node based systems but are much more difficult to circumvent. One drawback of using ISP level systems is that it is difficult to implement different levels of filtering to individuals as, typically, filtering is based on network addresses and not individual users. It is therefore difficult to enable adults in a household to access adult content while at the same time blocking the same content to children in the household.

2.2 Stopping Prohibited Content in the Internet

The Internet is used daily to transfer information of a sensitive nature in a secure manner. Security can be achieved in a number of ways and at different levels. The reality is that information on security is readily available in textbooks. It is therefore not difficult for a group of people to obfuscate and secure a system of content so it is only accessible to members of the group.

Discounting the addition of static content – i.e. content that remains accessible over a long period – the problem of filtering and detecting content created in real time is clear. A current trend is to put live TV and audio feeds on the Internet, both to residential broadband users as well as mobile devices. It is impossible to monitor all live feeds of video on the Internet and to censor such media in real time.

2.2.1 Impact of IP address and domain blocking

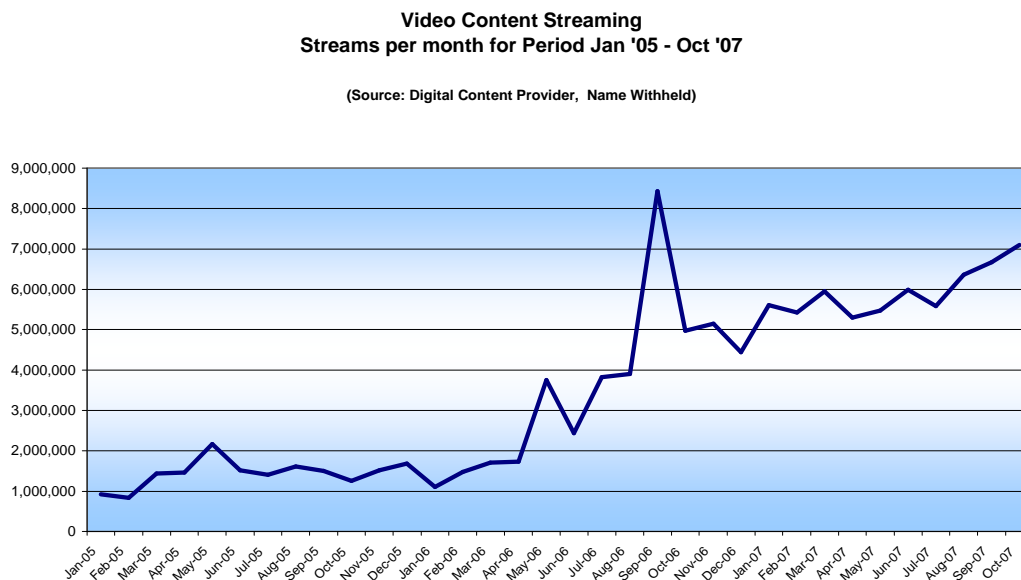
It is important to make a clear distinction between the content and its place of residence. Some techniques used for content filtering are based on IP addresses or domain names as identifiers. There is a risk involved in such coarse grained filtering. It is perfectly possible to host many websites on an end-node. If the content on one of the sites is prohibited or classified and the filtering is done based on an IP address, the other sites on the same host will also be blocked, even though there is no relationship

between the content providers. Similarly, many popular websites build on user-generated content such as web forums, Youtube, and Flickr. If a contributor adds prohibited or classified content to such a site and the filtering is domain name-based, the entire site will be blocked. The sheer volume of contributions to such sites (for example, every minute, **eight** hours of video is uploaded to YouTube [source: Google Australia]), makes scanning of content prior to posting impossible. It should be noted that normally such sites implement their own complaint-based censorship mechanisms where prohibited content is removed voluntarily by the site manager.

2.2.2 Impact of richer multimedia

Video content is steadily increasing on the Internet, as broadband connectivity becomes more easily available (source: a large national service provider. See Diagram 2.0).

Figure 8.0: Video Content Trend



This development has serious implications for the performance and feasibility of content filtering. It is computationally very expensive to filter video streams and to extract meaning so that content can be classified. In addition, the accuracy of feature extraction is typically very low unless the video and considered feature set follow stringent guidelines. Given current technologies it is not feasible to implement robust and meaningful video filtering systems and a large part of the Internet content has to be filtered manually for the detection of prohibited content.

3.0 Technical aspects of Dynamic Content Filtering

3.1 Overview of Dynamic Content Filtering

Dynamic content filtering builds on techniques often referred to as ‘Deep Packet Inspection’ techniques, where certain network nodes look at information embedded inside IP packets in order to make routing decisions, rather than looking solely at the information contained in the IP header itself. Such techniques are in widespread use on the Internet today; for example, they are used by some ISPs that want to identify certain application flows, such as Peer-to-Peer (P2P) file sharing traffic.

In the case of dynamic content filtering, identifying the application is not sufficient, as all content uses the same application – a web browser. Instead, the problem is shifted to inspecting the media itself and making decisions on what ‘class’ certain content belongs to. This includes extracting the text and image/video information contained on a web page.

This operation introduces a number of constraints on the platform that performs the inspection; for example, it is necessary to be able to store states between packets in flows and to cache content in each packet to be able to make a classification based on data in several packets. The computational processing required to perform the classification is well beyond the capability of a purpose-built router/switch and has to be done on a separate computational platform. This, in turn, translates into service providers having to make investments in purpose-built data inspection platforms.

3.2 Methods for content classification

There are a number of techniques for classifying content:

1. Natural Language Processing (NLP)

This represents the science of extracting information about the meaning of text from a given corpus.

An example of this is extracting information from medical records written by different practitioners for statistical analysis. It is inherently difficult for computers to capture human features in language, such as irony, as personal attributes are not easily modelled and do not follow clear patterns. The current state of the art in NLP can typically process text at a slow pace and with low accuracy.

Researchers at the University of Sydney have, in recent results, been able to parse text in the order of 1000 words per second with an accuracy of ~70 % in extracting correct meaning on a single representative PC. However, these results were based on a narrowly defined corpus in which texts adhered to a standard set by *The Financial Times* and were from a homogeneous group of authors. In the case of the content on the World Wide Web (WWW) the information is not standardised and the authors

represent a heterogeneous set. Bearing this in mind, the expected processing capacity and accuracy would be significantly lower with this corpus.

2. Data mining.

Data mining techniques are typically not used to extract semantic meaning out of sentences. Instead, these techniques are used to make classifications of data based on statistical properties.

The basic steps involved in this process include:

1. Organising the data in a form so that statistical properties can be gathered;
2. Gathering statistics, e.g. counting frequencies of words in a document;
3. Applying the classifier to the data to make the classification; and
4. Taking action based on the results.

In this context, the classifier is the crucial element, as steps 1 and 2 are reasonably straight forward, accurate and not computationally complex.

With the classifiers there is a fundamental trade-off between computational complexity (the time it takes to make the classification) and the accuracy of the classification, both of which are essential in the dynamic content filtering scenario. If the accuracy is high but it comes at the cost of large computational effort, the system requirements may be too demanding for ISPs to implement into their systems. Conversely, if the computational requirements are low but the accuracy is also low, there are serious implications in terms of the usefulness of the filtering.

3.3 Adversary actions and implications

It is evident that a change of policy to incorporate dynamic analysis will drive the adversary to make changes to circumvent the filtering system. For example, content based on text can be shifted to images that are inherently more difficult to decipher and in relation to which the computational complexity is significantly increased, or certain keywords can be used to lower the certainty of the classifier (e.g. the use of the term 'breasts' instead of 'tits').

Another example is the combination of smaller images to fewer but larger images on a page, as the image count is used as a distinguishing feature between pornographic and non-pornographic sites. It is therefore easy for the adversary to make the accuracy of the filtering significantly lower.

Even if an accuracy of close to 100% could be achieved using such simple and computationally viable filters there are significant implications for such a system. Because of the large volume of web requests there will be a significant count of false positives; i.e. web pages falsely classified as barred content. There are issues with unfair disadvantaging of the producers of this content from a legal perspective, and also the risk that desirable content is wrongly barred, such as information on sexual health advice, breast cancer and the like.

In addition, the only way of rectifying such wrongful classification is by human intervention and manual reclassification of content. Because of the enormous amount of information requested from web pages this is a serious resource issue. In addition,

there will be a significant lag in such rectification, leading to further competitive disadvantages for the affected content providers and to inaccessible information for the consumers.

SECTION F: INDEPENDENT LEGAL REVIEW

This part of the report provides a legal assessment of ISP level content modelling generally and the ISP management models specifically.

1.0 Independent Legal Assessment of Management Models

Each of the three management models was assessed by Freehills Solicitors to determine the legal risks to managers of the scheme and its participants. The full assessment by Freehills Solicitors can be found in Part 2, Appendix J. The authors of this report have prepared the following summary:

1.1 Differences between models

The nature of the legal risks that managers and participants may be exposed to are illustrated below:

1.1.1 Government

In general terms, the risk to the government is likely to be higher in the third party managed model and the hybrid managed model because in these models the government is responsible for ensuring that filtering is effective. It is likely that ISPs would seek to be indemnified by the government and/or filter operator for any claims made by users about the quality of the service provided under either of these two models.

1.1.2 ISPs

Risks to ISPs are likely to be higher in the ISP managed model, most significantly because ISPs in this model are responsible for both ensuring that their filtering solution meets the minimum required standard, and also for processing calls from users requesting the service. If an ISP has the capacity to provide the call centre service itself, the hybrid managed model may be seen by ISPs as of lower risk, as the ISP is not dependent on the performance of a third party in providing the service and managing personal information appropriately. Conversely, an ISP without that capacity may see the third party managed model as preferable. We understand, however, from a business perspective, that ISPs may prefer the ISP model despite the greater legal risks, because the operation of the entire system remains within its control to a greater extent than in the other models.

1.1.3 Users

When an additional party is added to operate the call centre, additional privacy risks arise in the handling of information about users. Privacy risks may therefore be lower in the ISP managed model and the hybrid managed model because each of these requires the user to continue to deal with their ISP, and not a new party (for example, a national call centre).

1.1.4 Outsourced service providers

Where a model involves outsourced services, as is the case with the call centre in the third party managed model and the filter service if the ISP outsources that function in the ISP managed model, additional risks may arise because the participants will be reliant on a third party to provide a service to the required standard. The nature of the legal risk that results will largely depend on the suitability and effectiveness of the underlying outsourcing agreement.

1.2 Service Specific Risks

1.2.1 Possession/distribution of illegal content

All states and territories and the Commonwealth have laws which prohibit the possession and distribution of some types of inappropriate content (for example, child pornography). These laws include, for example, sections 474.19 to 474.23 of the *Criminal Code Act 1995* (Cth) s 578C of the *Crimes Act 1900* (NSW) and section 70 of the *Crimes Act 1958* (Vic).

To the extent that the blacklist or vendor lists are made up of banned content under those laws, any person creating, amending and distributing the blacklist may risk breaching these laws.

1.2.2 Over-blocking and under-blocking

If a user of the blocking service is unable to access a web page that should not, in fact, have been blocked under the relevant criteria, their ISP, the national filter operator, and any relevant outsourced service provider, may have some liability.

The nature of this liability will depend on the precise nature of the arrangements; how the service is represented; and the terms of the relevant contracts. The nature and extent of this liability will also depend on whether the incorrectly blocked site was blocked because it was wrongly included in the blacklist (in which case ACMA may also risk some exposure, including for negligence or breach of statutory duty); was blocked by an inappropriate application of dynamic analysis or for some other reason, such as an error in the filtering system itself or in the delivery mechanism from ACMA to the filtering system.

The operators of the wrongly blocked site may also seek redress.

Similar exposure may arise for under-blocking (allowing access to content that ought to have been blocked).

1.2.3 Service degradation and breach of existing ISP contracts

ISPs have contractual arrangements with their users that will likely define the nature and quality of the service provided.

ISPs may therefore also breach their contractual obligations with users through, for example:

- A specific or general degradation of service as a consequence of the technical implementation of blocking; or
- Breach of contractual undertakings to not examine dataflows at the 'deep packet' level that may be required by some dynamic analysis.

1.2.4 Interception and hacking

The filtering aspect of any proposed model must be designed so that its operation complies with the communications protections in Part 13 of the *Telecommunications Act 1997* (Cth), the *Telecommunications (Interception and Access) Act 1979* (Cth) and federal, state and territory telecommunications and computer crime legislation.

A potential legal risk is that an entity providing any function could be liable as a result of the activity of a hacker successfully circumventing the system, or a user inadvertently circumventing the system by, for example, connecting via a Virtual Private Network (VPN) to an unfiltered office network.

Consideration could be given to the nature and extent of any protections that may be required as a consequence of anyone accessing illegal content through the methods defined above. Whether or not the entity would be liable would depend on a number of factors including: the terms of any relevant contracts; the consequences of the hacking; and the legislative framework. This risk may be greater in the ISP managed model because of the greater number of potentially differing approaches to filtering.

1.2.5 Freedom of expression

Any law proposed to implement the scheme as it is contemplated by the models would need to be structured to ensure that it did not infringe the implied guarantee of freedom of communication in the Australian Constitution. In summary, if the law placed limits on the freedom of communication, such limits would need to be appropriate to achieving a purpose within legislative power, and in a manner that is compatible with representative and responsible government. This risk is the same for each model.

1.2.6 Privacy

Privacy obligations will apply to most if not all managers under each model. These obligations include requirements to ensure that any information about individuals (personal information) is collected, stored, used and disclosed in accordance with the applicable privacy principles. Specific requirements include obligations to ensure that individuals are aware of how their personal information will be processed and by whom, and obligations to keep personal information secure and to ensure that it is accurate, complete and up-to-date.

Additional privacy risks and compliance complexity will arise to the extent that outsourced or external providers are employed to perform services that involve handling information about individuals (for example, the national call centre in the third party managed model and any outsourced filtering service in the ISP managed model).

1.2.7 Negligence

Whenever there are relationships between parties there is potentially a risk of negligence claims. There are a number of situations in which parties in each of the models might be exposed to the risk of an action in negligence. This may arise, for example, if a third party call centre fails to properly relay a request for blocking to an ISP, or an ISP negligently fails to act on such a request.

The nature of the risk will also be very dependent on how the filtering scheme is promoted – is it to be a guaranteed, ‘best efforts’ or no liability service?

1.2.8 Misleading conduct

Both the *Trade Practices Act 1974* (Cth) and state and territory fair trading legislation would impose obligations on managers (other than ACMA) to ensure that they did not engage in conduct that was misleading or deceptive in the provision of the blocking services, and that that did not mislead the public as to nature, characteristics or suitability of the services.

1.2.9 Sale of goods and provision of services

Similarly federal, state and territory legislation regulating the sale of goods and the provision of services may apply in order to imply terms into any agreements to provide ISP or filtering services. These terms may require that those services be fit for purpose; of merchantable quality; correspond with any description of the service; and that any services be provided with due care and skill.

1.2.10 More general issues

There is the potential for more general contractual breaches, including failure to deliver promised services. Each model contemplates contracts for the delivery of certain services. There will always be a legal risk relating to the provision of services as contracted and otherwise represented. Depending on the nature of filtering, contractual breaches may, for example, occur if the filtering is inconsistent with contractual promises.

Summary matrices set out by function and then by management model are available in Part 2, Appendix J.

SECTION G: CONSOLIDATION

This section of the report consolidates the results of the study against the agreed terms of reference.

- **Degree of difficulty in building a system**

Both the face-to-face interviews with ISPs and the responses to the questionnaire suggest that all ISPs regard filtering in general, and the implementation of any management model, to be a complex process. Many wholesale service providers saw themselves as being the ones who would ultimately apply any filtering solution, however they all thought the implementation would be complex (see page 45).

A key concern is the integration with existing infrastructure. *“Many felt that the requirement for handling user preference to opt-in or out of filtering would increase the level of complexity, in terms of technical architecture, business processes and customer support, and accordingly [this] will have large cost implications”* (see page 35). The questionnaire results suggest that over 90% of ISPs would find the implementation of a system to be either difficult or very difficult. This is regardless of the size of the organisation.

The filter vendors interviewed all have filtering mechanisms available, however any difficulties for them in providing a system revolve around how ‘blacklists’ are distributed, the format they are in, and whether filtering is based on exact or pattern matches (see page 39).

Strategic Implications

- Clear requirements are required by vendors to determine appropriate systems.
- Build impacts on ISPs need to be minimised to ensure efficient and effective implementations.

- **Likely performance impacts on the network**

The ISP industry was unanimous in the view that network performance would be impacted by dynamic analysis. The independent technical assessment suggests that this is also the case, primarily because of the processing power required to perform this type of filtering. *“The computational processing required to perform the classification is well beyond the capability of a purpose-built router/switch and has to be done on a separate computational platform”* (see page 61).

For blacklist filtering based on URLs, filter vendors suggested that *“in terms of performance impacts it is the act of inspecting traffic in order to obtain the URL that has the performance costs”* (see page 40). This corresponds with comments from the BT Cleanfeed Program where they estimate that the number of URLs would be *“in the 100’s of 1000s before service was affected”* (See Part 3, page 25)

For all content providers, broadband uptake and speed was seen as very important to their businesses: *“Broadband speeds in Australia are low and [content providers] are concerned about any scheme which degrades existing performance, particularly as it relates to video streaming, which has grown dramatically over the past 18 months. Speed degradation would seriously impact that growth”* (see page 38).

Strategic Implications

- Dynamic analysis is not feasible as a filtering method until/unless detailed testing and analysis is undertaken on the network performance impacts. Any such testing would need the support of ISPs and should also consider the impacts on new and emerging technologies and usage trends.
 - The parameters of URL based Blacklist filtering would need to be determined and then tested to determine network performance impacts. Any amendments could then be made accordingly.
- **Time needed to build the new system**

This term of reference was dealt with through the questionnaire. The majority of respondents thought that filtering would take up to one year to implement.

Strategic Implications

- A minimum period of one year would be required by industry to implement any filtering system and should be factored into any requirements.
- **Effectiveness of filtering and ease of maintaining current blacklists**

Most ISPs are not supportive of ISP level filtering. ISPs, vendors, the independent technical expert and previous studies all conclude that any filtering mechanism can be circumvented by those motivated to do so. Many tools for circumvention are freely available (see page 23). The potential for circumvention raises a number of legal risks, in particular, commercial liabilities (see page 67).

Amongst content providers and ISPs there was more general support for a human generated blacklist (see page 37). However, the level of awareness of the ACMA blacklist generation process amongst end users, in particular, was thought to be low (see page 36).

In terms of maintaining current blacklists, in Canada the review of blacklists occurs on a weekly basis through the use of automated systems that flag any URLs that have had content changes, and those flagged are reviewed by the analysts (see page 49). This appears to be potentially more effective and less complex than the current ACMA method of blacklist review: “ACMA has updated the blacklist on an ad-hoc basis to remove URLs that no longer resolve to prohibited/potentially prohibited content” (see Part 2, Appendix L, page 122).

Strategic Implications

- Consideration needs to be given to the nature and extent of any protections that may be required as a consequence of anyone accessing content through, or as a consequence of, deliberate circumvention of a filtering scheme.
- Should ISP level filtering be implemented, a public awareness campaign on the blacklist creation process should be considered.
- Consider an automated model as an option for review of the ACMA blacklist.

- Develop requirements for the evaluation, implementation and management of an appropriate authority for providing blacklist details to ISPs.
- **Effectiveness of and impact on network performance of filtering using URL-based blacklists (e.g. ACMA or vendor-maintained), dynamic analysis, or a combination of both.**

The RMIT study undertaken in 2006 suggested that the use of server based Internet content filters could impact on network performance (see page 25). The face-to-face interviews and the questionnaires undertaken with the ISP industry clearly indicate that ISPs are of the view that network performance would be adversely impacted by dynamic analysis (see page 34). This is supported by independent technical expert analysis, which concludes that dynamic analysis introduces a number of constraints on network platforms (see page 62).

With regard to URL-based blacklist filtering, the ISP industry has moderate concerns about the ACMA blacklist and strong concerns with vendor-maintained lists on network performance (see Part 2, Appendix F, pp.58-59).

Content providers expressed concern about the impact on their business if filtering reduces network performance and retards enhanced broadband speeds (see page 38).

In terms of effectiveness there was a general scepticism about the accuracy of filtering techniques using computer-based analysis (typically, vendor-maintained lists and dynamic analysis), (see page 33).

Strategic Implications

- Further detailed study should be conducted to quantify the performance impacts of different filtering techniques at an ISP level (note: the RMIT 2006 study was at the server level only).
- When developing the requirements for filtering it needs to be considered that the accuracy of the analysis of content (i.e. its classification) and the accuracy of filtering techniques and subsequent implementations are all distinct components of filtering.
- **Extent to which it (filtering) would interfere with normal business operations**

Some ISPs expressed concern about the competitive and commercial impacts that significantly large wholesalers would be able to impose on their resellers, particularly if their wholesalers introduced filtering on their behalf (see page 32).

At least one large ISP made the point that filtering would not be commercially advantageous to them: *It will not offer, in terms of ability to leverage mandatory filtering solutions, any advantage to the business and would not permit businesses to personalise their offerings*” (see page 34).

Nearly all ISPs believed that there would be additional customer support requirements with filtering, over and above normal business operations. Typically, this would require additional infrastructure (see page 36).

Strategic Implications

- The relationship between wholesale service providers and retail ISPs needs to be considered when formulating requirements for filtering, particularly any competitive and contractual issues.
- Awareness of the potential impacts of filtering on the 'end user' experience may need to be communicated so that expectations can be set.
- **Legal risks to managers of the scheme and the participants**

A number of legal issues and risks have been identified. Specifically those of:

- Illegally possessing or distributing illegal content;
- Over-blocking and under-blocking content;
- Service degradation and the potential impact on existing service level agreements;
- Interception and hacking;
- Impairing freedom of expression;
- Privacy breaches;
- Contractual claims;
- Negligence;
- Misleading conduct; and
- Breaching sale of goods legislation.

These issues and risks exist in performing the function of filtering as well as with the three management models proposed for consideration (see Part 2, Appendix J).

Issues of liability between parties and the impact of filtering on service level agreements were raised as matters of concern by ISPs – *“They felt that speed, reliability, scalability would be outside their control and outside of normal contractual arrangements, especially any service level agreements”* (see page 32) – and by content providers – *“Concerns were expressed by all about filtering using dynamic analysis specifically and computer based analysis generally because of the risk of false positives”* (see page 37).

For ISPs the audit requirements of a filtering regime were flagged as a matter of concern (see page 36).

In Europe a number of legislative changes have been implemented to protect ISPs from liability for content posted on their networks by third parties, the exception being illegal content (see pp; 42 & 48).

Concerns have been raised in Europe about having publicly accountable procedures for the creation and provision of blacklists (see page 43).

Strategic Implications

- Legal and procedural issues need to be addressed before a decision can be made on a filtering implementation for Australia.
- The overseas experience, particularly in Europe, can be used as a benchmark for addressing many of the issues likely to arise in Australia.

- **Likely build and maintenance costs**

A report by the CSIRO, *Blocking Content on the Internet*, 1998, flagged the likely high costs of filtering. “*The report noted the likely high cost of filtering, recognising that ISPs might not have the capital to invest in the hardware required and that they might not be in a financially secure position to spend money on ongoing maintenance and training costs for staff maintaining the filtering system*” (see page 24). The 2006 RMIT study on server-based Internet filters also concluded that: “*costs ... would not be small for large deployments*” (see page 25).

There is a general expectation amongst ISPs that the build and maintenance costs of filtering will be high. One ISP stated, during a face-to-face interview that “*the imposition of any additional government regulation will make their dial-up service no longer financially viable*”; they would “*discontinue it as a consequence*” (see page 35). Another ISP estimated that the cost of hardware to examine all the protocols of network traffic was “*between \$2-3 million*” (see page 35). There is concern amongst some ISPs that the additional amount of logging required to meet likely audit requirements would impact systems costs (see page 36). In terms of the management models, the questionnaire results show that the ISP managed model was seen as having the highest build and maintenance costs (see page 45). Across the board, all ISPs saw dynamic analysis as having the greatest impact on build and maintenance costs (see Part 2, Appendix F, page 57).

BT Cleanfeed provided an estimated cost of approximately £500k (circa \$1.5million Australian Dollars) for the development of their current system (see Part 3, page 26). This is a filtering system operating only within the BT network environment. Ultimately, final costs, and any subsequent impacts, can only be determined once the requirements of an ISP filtering system are known.

Strategic Implications

- The expected cost impact of any filtering implementation is such that cost recovery models should be a key consideration.
- Detailed requirements are necessary to produce a true estimate of costs and should be developed to assist with the cost modelling process.

- **Customer support requirements (initial and ongoing)**

There is a general view amongst ISPs that educating customers on the opt-in functionality in particular would be a “*large and costly endeavour*” (see page 35).

A commonly held view amongst ISPs was that regardless of whether or not filtered customers were directed to call a third party, “*users would still call their ISP at some point, if only for an explanation*” (see page 36). In general, this would be an ongoing issue.

Content providers also saw that customer support requirements were likely to increase in that inadvertent filtering, “*particularly if sites linked to their sites were filtered ... would cause confusion in the user and increase [the need for] support calls to inform*

them that the link on their site is wrong or to question why they were linking to a site that is prohibited” (see page 38).

The questionnaire results highlighted that all ISPs regard their relationship with their customers as paramount (page 44).

Strategic Implications

- Increased call volumes can be expected by ISPs primarily, and secondarily by content providers. This should be factored into cost recovery models.
- Detailed requirements that provide specific customer service information will assist ISPs and content providers with any customer support planning requirements.
- The importance of maintaining the customer relationship needs to be considered when developing the objectives and requirements of filtering.

• **Administration costs (initial and ongoing)**

ISPs felt that the costs would be much greater for a filtering scheme where customers must opt-out, rather than opt-in. This was because with *“opting out it would be necessary to scale systems for 100% of users, whereas with opting in, it was highly likely that only a small percentage of users would select this option, thus systems could be scaled accordingly”*. More than the cost of systems, ISPs also considered that with opting in there would be greater staff requirements (see page 35). The questionnaire results showed that ISPs clearly envisaged increased administrative costs – both initial and ongoing – with filtering using dynamic analysis (Part 2, Appendix F, page 56).

One content provider also envisaged additional administrative costs with the opt-out model, stating that it would *‘add costs’* and may mean that *‘labelling would be less honest’* (see page 36). Typically, content providers saw increased administrative costs arising through incorrect filtering, creating the need *“to contact the ACMA (or relevant authority) to unblock sites/pages”* (see page 38).

The Ovum Report 2003, identified costs for government of filtering, including the *“promotion and enforcement of filtering and maintenance of an authorised blacklist”* (see page 25).

Strategic Implications

- The opt-out scenario requires more detailed analysis and definition before being considered as an implementation option.
- A cost effective and efficient complaints process for industry would need to be developed and implemented, preferably in consultation with industry, to help reduce the administrative costs of filtering.
- A cost recovery model for any filtering implementation incorporating dynamic analysis would need to be given serious consideration.

- **International precedents and the nature and extent of options employed elsewhere.**

There are a number of ISP-based national filtering implementations, predominantly in Europe (see page 47). In almost all instances the filtering is voluntary and in some jurisdictions, such as Germany, is not enforced. The methods and technologies used to apply filtering are greatly varied, from DNS blocking to URL filtering. There is a no clear preference between Domain Name System (DNS) filtering or URL filtering. In some countries there are no agreed methods of implementation, with the method for implementation being left to the discretion of individual ISPs (see page 42).

In general the list of URLs (sites) to be filtered are sourced from law enforcement; some are sourced from government departments, Non Government Organisations (NGOs) and other sources.

The common factor amongst the international filtering implementations is child protection through the removal of child abuse images (see pp.47-50).

Strategic Implications

- International precedents exist for implementing filtering in the Australian context (in particular the filtering of child pornography).
- The international implementation methods, legislative models and objectives for filtering can be used as benchmarks for any Australian implementation.

- **Identification of likely barriers to compliance across whole of industry**

The Ovum Report 2003 identified annual recurring costs, such as “*initial set up costs [equipment and staff to install and configure] and annual recurring costs [software licenses, support staff]*” (see page 24). The report stated that the impact on small ISPs would be more significant than on larger ISPs. Having access to the capital required for the initial set up costs and for the ongoing operational expenses is potentially a barrier to compliance, predominately in the case of smaller ISPs but also across the industry.

Strategic Implications

- Financial support may be required by ISPs for the initial establishment of filtering.
- Cost recovery models for ongoing expenses also need to be considered.

- **Impacts likely to apply disproportionately across industry.**

A disproportionate impact was identified amongst user-generated content providers. They were identified as being most at risk of inadvertent filtering. User-generated content is growing significantly hence, this impact is of concern (see page 37). Typically, amongst younger people “*from age 14 onwards, 70 per cent or more of teenagers are engaged in some form of web authorship*” (see page 22).

Any implementation of ISP level filtering beyond a blacklist implementation may also have a competitive impact on existing Australian ISPs that undertake ISP level content filtering (see page 50).

The questionnaire results clearly indicate that the smaller ISPs are most likely to be impacted with any filtering implementation as a result of resource constraints. For obvious reasons, resource constraints are less of an issue in larger organisations (see page 45).

Strategic Implications

- Industry reporting and complaints procedures need to be defined and established. A communications plan then needs to be developed and advertised to ensure that user-generated content providers are aware of requirements.
- Financial support may be required by ISPs for the initial establishment of filtering.
- Consider establishing a body or group designed to provide specialist advice and support to ISPs to assist with any filtering implementation.

SECTION H: ISSUES & RECOMMENDED NEXT STEPS

This section of the report outlines the issues that require further consideration.

1.0 Issues for consideration

Based on the 'Terms of Reference' and the results of the study the following issues have been identified. Whilst extensive, the final strategy, once known, will likely produce a more comprehensive list of issues to be addressed

1.1 Possession and distribution of illegal content

Specific issues to be addressed in this regard include:

- Whether the URLs or other identifiers of banned material on the blacklist or vendor lists are themselves banned material, and whether consequential legislative changes might therefore be required prior to implementing a model is based on any wider distribution of or involvement in the blacklist than is presently the case under the *Broadcasting Services Act* Schedule 5 scheme;
- Whether any additional statutory or other protection may be necessary for employees, contractors or consultants involved in the process; or in the case of employers, to protect them from potential actions by employees, contractors or consultants with respect to their exposure to the material; and
- The nature and extent of any security requirements and indemnities with respect to the handling, transfer and publication of the blacklist and vendor lists.

This risk exists in all models but in the ISP managed model the risk may be more significant as that model involves independent parties providing the filtering service.

1.2 Technical Solution

- All systems will in some manner be circumventable

It is important to understand the limitations of any proposed system so that expectations, particularly within the general public, are realistic. Some pertinent questions are:

- What circumvention techniques have already been identified?
- How can we discover additional techniques?

It is possible to circumvent IP filtering and URL filtering using a number of techniques, some as simple as using an anonymous proxy website (which, on behalf of the user, requests another web page and returns it to the user); language translation sites (which are similar to an anonymous proxy except that they translate the web page into another language before sending it back to the user); or as straightforward as accessing a SSL version of a website. Such techniques are available to anyone already using the web.

Other techniques, which require the use of software, are also available, such as tunnelling.

- Discretion on level of filtering

There might be a minimum level of filtering that is required, such as a predetermined blacklist of URLs that must be filtered. Will those implementing the filtering solution be given the discretion to implement as they see fit provided they meet the minimum level? If so, an ISP might choose the cheapest method of filtering which results in potential 'collateral damage', such as sites not on the blacklist being filtered.

- Length of time to implement

Having a reasonably informed estimate of the amount of time it will take to implement a mandated filtering solution (including, design, installation and testing), will ensure that any compliance deadlines imposed on ISPs are reasonable and provide enough time to do what needs to be done, without adversely impacting on quality.

- Impact of mandated filtering on existing ISP implementations in Australia

In Australia there are some ISPs that currently offer a filtered Internet service to their customers. The impact of a mandated national service on their business model would need to be considered.

- Costs

The cost of building and offering a filtered Internet service could involve the following:

- Designing the system
- Procuring the equipment
- Purchasing software
- Installation staff costs
- Operational support staff
- Ongoing software licenses
- Equipment and/or software upgrades
- Support contracts

These would all need to be considered in any cost model.

- System design requirements

Some key factors that will need to be considered when implementing a filtering system:

- Scalability
- Redundancy
- Size
- Throughput

- Functionality
- Reliability
- Cost
- Support requirements

- *Level of testing*

Every system should be subjected to a different regime to ensure systems quality. Commonly, testing is the responsibility, and performed at the discretion, of those deploying the system. To ensure quality of filtering throughout Australia it might be advisable to establish some service levels that must be met. Doing so would encourage testing. Setting minimum service levels, however, would require systems to track service level performance. This would be an added cost to those responsible for the filtering system, not to mention an extra cost to the monitoring body.

- *Scope creep*

There is a concern that once filtering systems are in place there will be pressure to push for an increase in the breadth of filtering. It is important to understand that systems are designed based on detailed requirements. Changing the scope (the details) means changing the system.

- *Confidentiality*

The design of the system will need to consider confidentiality of the list and ensure that it is transferred to the filtering system securely and that the system itself is secure as much as is possible.

- *Acceptable performance impact*

The major concern of ISPs and digital content providers is that filtering may negatively impact network performance; for instance, by increasing latency. It is reasonable to expect (see previous studies) that content filtering will slow down network speeds to some extent.²¹ Such a concern highlights the necessity to decide upon what, if any, performance impacts are acceptable, and who would determine such standards (i.e. the Australian public, or ISPs, or both?).

1.3 Management Models

- *Existing models*

Experience already gained locally and overseas should be considered. At least one overseas ISP (BT) is already deploying a filtering system on a large scale, and is prepared to offer expertise and assistance with infrastructure design to ISPs in Australia. Feedback on the experiences of those already using a filtered Internet service may provide valuable insights.

²¹ Note: The ACMA Tasmanian trial will also provide data relevant to this issue.

- Wholesaler implemented

In the UK about 20 million Internet connections are now filtered, and the filtering is performed by the wholesale service provider. Would this work in Australia? The legal and competitive issues of such implementation need to be considered.

- Where responsibility lies

A crucial question for most ISPs is where the responsibility will lie when it comes to filtering, and what that responsibility will be. For example, who bears the responsibility in terms of the quality of filtering, reporting related to filtering, etc?

- Managing the customer preference

If a national hotline was established that customers call to opt-in or out of filtering, the following questions should be considered:

- Who can call?
- How will users be identified (as customers of such and such ISP)?
- How long will the user's preference take to be communicated to the ISP?
- By what method is it communicated?
- Does a person with multiple ISP accounts need to request filtering on each account?
- Will the hotline be open 24 hours a day, 7 days a week?

- Industry convergence

Mobile service providers are now offering Internet access to their customers through mobile phones or other handheld communication devices. Consideration should be given to how mobile carriers differ from traditional ISPs and whether they should be required to comply.

1.4 Filtering – what to filter, how to maintain it

- What traffic to filter

There are many types of traffic on the Internet. Some popular types are web traffic, email, VoIP, audio and video streaming, instant messaging (MSN, Yahoo) and peer-to-peer. What type of traffic is it intended should be filtered?

It has been suggested that blocking web pages may not be sufficient to protect children; for example, Internet chat rooms, instant messenger services or social networking sites such as MySpace will also need to be considered.

- Level of Accuracy

When content is found to be prohibited in a URL filtering scheme, typically, the exact URL of that content is added to the blacklist. In some cases, filtering based on an exact URL might not be desirable. For instance, the URL of the web content changes frequently (although it stays on the same site). In such a case, filtering the whole site might be more prudent. Doing so, however, will impact on the design of the filtering system. Noteworthy is the fact that filtering based on non-exact URLs increases the risk of collateral damage.

- Size of the list

The maximum number of URLs that a blacklist can contain is an important factor in system design. Having no limit means that the blacklist could grow indefinitely and thus, impact the ability of ISPs to scale systems appropriately and potentially the filtering techniques.

- Limits on what to filter

A large concern with filtering is that over-blocking will occur. Some filtering techniques will produce larger levels of over-blocking than others. Should certain filtering techniques (e.g. IP and DNS filtering) be expressly prohibited with any mandated filtering scheme?

- Compilation of the list of content to filter

How should review and classification of content be conducted and by whom?
What resources (type and number) will be required to compile and manage a central list, particularly a human generated blacklist ?

- Computer-based categorisation/classification

For computer-based categorisation some key issues for consideration are:

- What are the possible categories of classification and who determines them?
- What are the criteria and processes used for each classification and who determines them?
- What minimum level of accuracy is required before the computer-based classification is acceptable, and who decides that level of acceptability?

- Blocking new content

In an ACMA or vendor list based filtering scheme, once it has been decided that particular content should be blocked, the URL of that content needs to be communicated to the filtering system as fast as possible. The type of communication mechanism needs to be determined and offer consistency across all ISPs to ensure a rapid deployment of 'unacceptable' sites.

- Central list server

Distribution of a blacklist in a secure manner to the 700 plus ISPs in Australia will not be trivial. Any data retrieved from a centralised server must be dealt with in a secure manner. The details will need to be determined on how the list is retrieved, who is authorised to retrieve it, how authorised users verify their identity, in what format the list will be in, how often to retrieve it, how to know if the list has changed, how to know that retrieval of the list is successful, and more.

Maintenance of the systems infrastructure for the central server is crucial as well. It will need to be redundant, highly secure, and changes to external interfaces will need to follow very clear processes so that third parties (e.g. ISPs) are notified of impending changes. Likely, too, will be the necessity of some level of auditing of the activity of that server. Review of that audit information will detect security breaches, hack attempts and even non-complying external parties (i.e. ISPs not retrieving the list as required).

- List security

A blacklist has the potential to become valuable in its own right. There may even be attempts to reverse engineer the blacklist.

(Reference: www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf)

The security and secrecy of a blacklist will need to be safeguarded; it will need to be stored securely and communicated securely. Parties legitimately receiving copies of the list should be obliged to implement procedures to keep it secure.

Consideration needs to be given as to who should be privy to the blacklist in any organisation.

At least one ISP emphasised that putting a secure blacklist in the hands of every ISP in Australia is almost certainly going to mean that the blacklist will leak.

Clarifications on the handling process and on who may actually handle the list, at the ISP level, are therefore required.

- Limitations to exact URLs

Some sites now use auto-generated URLs for each page and so a blacklist of exact URLs would be almost meaningless for those sites. It would therefore be more effective to block the whole domain but with that comes the risk of 'collateral damage'.

- When filtering occurs

Should users know when the content they attempted to access was blocked? That is, by displaying a 'blocked' page, rather than just making the requested web content non-existent (i.e. through a '404 – page not found' error message).

If a blocked page is displayed it is necessary to decide what it will say. It will also be necessary to decide who determines the message content and where the page will be hosted.

- Consistency of filtering

Does filtering need to be consistent across all ISPs? If so, then the following points are relevant:

- A predefined list of URLs to filter, distributed from one source to all parties implementing filtering, will provide consistency.
- Permitting parties to choose their own vendor list will not provide consistency.
- Computer-based analysis of web content will by its very nature mean that there will be no consistency unless every party uses the same computer-based analysis system with the same parameters.

- Systems failure

As with all modern systems, disaster plans are required to be developed before disaster strikes. How faults are reported and what actions are taken are critical issues in minimising the impact of the disaster. One evident eventuality, in the context of ISP level filtering, is that the filtering system stops working. What should occur then? Should all web requests go through unfiltered or should they all be blocked?

There should be planning for each element of the scheme, including such disasters as the central filtering criteria server being hacked, the security of audit information being compromised, and many other like scenarios.

- Greater granularity

Some ISPs and digital content providers suggested that it might be preferable to offer multiple levels of filtering - more than a simple 'on' or 'off' system. Users would have more control of their filtering and it might be clearer to users what is being filtered. Google safe-search was given as an example, in which users have the choice of "no filtering, filtering of explicit images only [the default setting], or filtering of both explicit text and explicit images".

(Reference: <http://www.google.com/preferences>)

1.5 Legal

- Prohibited content

Will content be prohibited under Schedule 5 or 7 of the *Broadcasting Services Act* 1992?

- Illegally possessing or distributing illegal content

Are the URLs or other identifiers of banned material on the blacklist or vendor lists themselves banned material, and might consequential legislative changes therefore be

required prior to implementing a model that necessitates any wider distribution of, or involvement in, the blacklist than is presently the case under the *Broadcasting Services Act* Schedule 5 scheme?

Are any additional statutory or other protections necessary for employees, contractors or consultants involved in the process; or, in the case of employers, to protect them from potential actions by employees, contractors or consultants with respect to their exposure to the material?

What is the nature and extent of any security requirements and indemnities with respect to the handling, transfer and publication of the blacklist and vendor lists?

- Over-blocking and under-blocking

If a user of the blocking service is unable to access a web page that should not, in fact, have been blocked under the relevant criteria, their ISP, the national filter operator and any relevant outsourced service provider may have some liability. The nature and extent of this liability will also depend on whether the incorrectly blocked site was blocked because it was wrongly included in the blacklist (in which case ACMA may also risk some exposure, including for negligence or breach of statutory duty); whether it was blocked by an inappropriate application of dynamic analysis, or for some other reason, such as an error in the filtering system itself or in the delivery mechanism from ACMA to the filtering system

The operators of the wrongly blocked site may also seek redress.

Similar exposure may arise for under-blocking (allowing access to content that ought to have been blocked).

- Service degradation

ISPs may breach their contractual obligations with users through, for example:

- A specific or general degradation of service as a consequence of the technical implementation of blocking; or
- Breach of contractual undertakings to not examine dataflows at the 'deep packet' level that may be required by some dynamic analysis.

- Interception and hacking

The filtering aspect of any proposed model must be designed so that its operation complies with all existing legislation that places obligations on such things as:

- Requirements on carriers and carriage service providers and their employees to protect the confidentiality of information relating to the contents of communications carried, carriage services supplied and user's affairs or personal particulars;
- Prohibitions on the interception of telecommunications; and
- Prohibitions on unauthorised modification of data and unauthorised impairment of

electronic communications.

Consideration could be given to the nature and extent of any protections that may be required as a consequence of anyone accessing content through, or as a consequence of, deliberate circumvention of the scheme.

- Impairing freedom of expression

Any law proposed to implement a national ISP level content filtering scheme would need to be structured to ensure that it did not infringe the implied guarantee of freedom of communication in the Australian Constitution. In summary, if the law placed limits on the freedom of communication, such limits would need to be appropriate to achieving a purpose within legislative power, and in a manner that is compatible with representative and responsible government.

- Privacy breaches

Privacy obligations will apply. Such obligations will include requirements to ensure that any information about individuals (personal information) is collected, stored, used and disclosed in accordance with the applicable privacy principles. Specific requirements include obligations to ensure that individuals are aware of how their personal information will be processed and by whom, to keep personal information secure, and to ensure that it is accurate, complete and up-to-date.

- Contractual claims

There will always be a legal risk relating to the provision of services as contracted and otherwise represented. Depending on the nature of filtering, contractual breaches may occur, for example, if the filtering is inconsistent with contractual promises.

- Negligence

There are a number of situations in which parties in each of the models might be exposed to the risk of an action in negligence. For example, if a third party call centre fails to properly relay a request for blocking to an ISP, or if an ISP negligently fails to act on such a request. The nature of the risk will also be very dependent on how the filtering scheme is promoted – is it to be a guaranteed, ‘best efforts’ or no liability service?

- Misleading conduct

Current legislation exists to ensure that those offering filtering services do not engage in conduct that was misleading or deceptive in the provision of such services and that they do not mislead the public as to the nature, characteristics or suitability of the services.

- Breaching sale of goods legislation

Similarly federal, state and territory legislation regulating the sale of goods and the

provision of services may apply in order to imply terms into any agreements to provide ISP or filtering services. These terms may require that those services be fit for purpose; of merchantable quality; correspond with any description of the service; and that any services be provided with due care and skill. Service level maintenance has the task of ensuring that ISPs' day-to-day service to users is not degraded by filtering to an extent that is legally unacceptable.

- *Public access*

The *Freedom of Information Act 1982* has been used in the past to seek access to the ACMA blacklist. In the future such challenges may occur again, and might be in order to seek information on infrastructure design or other aspects of system design.

- *Right of appeal*

A major concern highlighted by digital content providers is that there need to be clear avenues of appeal for challenging filtered content. There needs to be clear rules on who can make such an appeal: should it be the content owner, the content host, the content publisher, including the organisation or person that provides the facility for users to publish their own content (e.g. sites such as www.blogger.com and www.youtube.com)? In the case of the ACMA blacklist, for instance, each URL on the blacklist would need to have a date of review, at which time a process is initiated to check if the URL is no longer active or the content has changed.

- *Further factors*

The way in which the effectiveness of the filtering service is described and promoted (particularly to end users) will be a critical factor when assessing legal risk. For example, is it promoted as a guaranteed filter of inappropriate material as opposed to a 'reasonable endeavours' type proposal to block that material?

The extent to which ISPs, the national filter operator, any third party vendors and ACMA will accept liability for the services they provide is not known. Some providers may, for example, provide services only on a 'best endeavours' or no liability basis.

1.6 Social

- *Public interest in filtering*

Has research on the end user perceptions of filtering been conducted at a government level? Such research might assist with developing objectives and subsequently requirements for any filtering regime.

- *Oversight*

An ISP level filtering scheme requires mechanisms to provide oversight of items such as list generation and maintenance and handling of compliance/audit information. An

example might be a body, government or otherwise, that is established to review decisions as to what is on the blacklist and to ensure that a transparent process for producing filter lists is in place.

- Supporting Australian industry

There are Australian vendors of filtering technologies. There are also many overseas-based vendors. Will a filtering scheme explicitly or implicitly support Australian industry or, alternatively, will Australian industry be adversely impacted?

- Disproportionate impacts

Will filtering only overseas-hosted content have the potential for greater impact on some Australian content providers, specifically those Australian content providers who have their content hosted overseas, rather than those who host exclusively in Australia?

- Adult content

The ACMA blacklist currently defines content that is classified X18+ as prohibited. This is a very broad classification that captures content such as non-violent erotica. If the objective of the filtering scheme was to block access to child pornography based on the ACMA blacklist, then this would need to be specifically stated in any implementation to reduce potential cross industry impacts.

- Education campaigns

As any filtering regime is able to be circumvented, establishing expectations as to what can be expected from any filtering regime may need to be considered.

1.7 Compliance and Auditing

- Proving compliance

ISPs (or third party filtering providers) will need to know the compliance requirements. Details, such as the following, will need to be defined:

- The precise information that will need to be reported.
- To whom to report the information.
- How often to report the information.
- The format in which the information needs to be reported.
- The mechanism used for transferring the information.
- Whether copies of the information needs to be stored, and for how long.
- The security procedures for storing and transferring the information.

The greater the level of auditing required, the greater the cost impacts.

- Use of audit information

The type of data required and the distribution of such information will need to be carefully considered. The greater the level of detail required for audit data, the greater the privacy impacts are likely to be.

- Auditing body

To ensure privacy, procedures will be required to restrict access to audit data.

In drawing up policies and procedures for this data, defining who should have access to the information, why, and what will they do with the information will be necessary.

- Confirming the user

Viruses and the wide variety of users on any computer system mean that obtaining forensically sound logs will be very difficult. In this environment, how will enforcement be applied?

- Scope of compliance

A decision will be required on the scope of compliance with a filtering regime. For example, will owners of Internet cafes, managers of Internet access in residencies, hotels, resorts, conferences, satellite Internet service providers or even owners of unsecured wireless access points, be included in list of organisations required to offer a filtered Internet service?

- International Internet access

There are likely some users in Australia who obtain their access to the Internet from outside the country. It could be through dialling internationally to a foreign ISP or through using a satellite service offering foreign Internet access. How will filtering be applied in this case?

- Audit data

Will audit data be used by law enforcement agencies? If so, this will require specific systems and business process design.

1.8 Financial

- Cost recovery

Government funding of any mandatory scheme should be considered to ensure that the industry does not have to bear the total cost of implementing the scheme.

- What the costs will be

There will be initial costs and ongoing costs related to the filtering system itself, as well as to managing customer preferences. What costs specifically can and will be funded?

Some likely initial costs may include:

- Equipment purchases
- Hiring expertise to design and install
- Licensing
- Call centre
- Administrative changes
- Internal business system changes

Some likely ongoing costs may include:

- Customer support
- Technology upgrades (up-scaling and keeping up-to-date)
- Equipment replacement
- Staff training
- Compliance processes and compliance processing activities
- Complaints investigations
- System maintenance
- Customer support costs.

ISPs have expressed concern that there may be other costs related to the operation of such a filtering service that will be harder to quantify, such as potential impacts to brand value – especially with erroneous filtering - and performance related issues.

Many smaller ISPs will not have adequate in house technical expertise with which to set up and maintain any filtering solution, and will need to bear the cost of outsourcing any solution developments.

- Reporting

What will be the government reporting requirements that must be met by ISPs?

Generally, the more extensive and detailed the reporting requirements, the greater the impact on IT systems development, maintenance, and hence cost.

- Cost of user preference

What would be the obligations of government if only a very small number of users opted out, especially if this occurred after ISPs had incurred additional cost to implement a practically unused system feature (i.e. user opt-out)?

1.9 Customer support

This is a large area with many impact points on ISP contributing to substantial cost.

Including the:

- Cost of setting up user preference handling (call centre training, customer relationship management systems, changes to billing systems).
- Ongoing cost of handling user preference (via call centre or website).
- Ongoing cost of handling user complaints and questions about filtering.
- Ongoing cost of call centre training on filtering.
- Ongoing cost of handling compliance related matters (including complaint investigations).

Management of these particular cost impacts, given the importance of customer relationships with ISPs (see Subsection 3.1.2), will need to be considered.

- Support requirements

How will users be verified when opting in or out of ISP filtering?

- Complaints process

A very clear process will need to be put in place to handle complaints about over-blocking, under-blocking and for challenging the legitimacy of web content that is blocked.

- Call centre impacts

It is thought that initially the number of support calls to ISPs will be large; in terms of the volume of ongoing calls, the number will reduce but will still be significant. The level of impact on ISP call centres will depend on a number of factors, such as reliability of the system to be implemented, usability, etc. User testing of such functionality is likely to be necessary, regardless of whether a mandated national filtering scheme, or an opt-in/opt-out scenario is deployed, so that impacts are fully understood.

- National hotline

With a national hotline, as envisaged as a component of the third party managed model, the level and quality of advertising of the hotline and the associated filtering scheme will impact customer support requirements and must therefore be carefully considered and structured.

- External filter provider

If filtering is performed by a third party, an extra communications channel will be required between the ISP and that third party for operational support and complaints management. The costs of this channel and the impact on smaller ISPs would need to be considered.

- User experience

To minimise business impact it will be necessary to ensure a positive user experience of filtering. This needs to be carefully defined and considered when selecting filtering methods.

1.10 Anti-Competitive Practices

Given the structure of the Australian ISP industry and the predominance and influence of a few very large players, care will need to be taken, when determining any requirement, to minimize the opportunity for anti-competitive practices (both technical and pricing). Specific attention may be required for VoIP services.

The convergence of technology, and the ability of the Internet to carry services like voice communication, creates a new paradigm for telecommunications. An assessment of the following may be beneficial in the development of future telecommunications strategies:

- The cross industry impacts of emerging technologies,
- The role of ISPs in providing traditional telecommunications services

2.0 Recommended Next Steps

As a result of the findings and comprehensive analysis we recommend the following next steps be given priority:

- Define the objectives of filtering;
- Consider applying the above objectives to a national filtering scheme with particular attention to be given to:
 - The role and scope of a filtering scheme;
 - The implementation options: i.e. ISPs either implementing their own filtering capability or utilising a national filtering service (refer to **Key Finding 4**).
 - The blacklist sources. International sources, such as INHOPE or the Internet Watch Foundation might be considered in conjunction with the ACMA blacklist;
 - The opt in/opt out framework. In particular, consider the implications of making the framework *optional* for ISPs;
 - The implications of making the national filtering scheme *voluntary* for the ISP industry, in line with international precedence.
- Engage with industry to clarify how such a scheme would:
 - Interface with existing ISP infrastructure;
 - Impact on broadband performance;
 - Impact on costs;
 - Handle the issue of recovery of costs to industry as a result of implementation.
- Undertake analysis to determine how vulnerable a national filtering scheme is to circumvention and to attempts to disable it.

- Consult relevant stakeholders regarding the management of the nationwide scheme. Issues to consider include:
 - The legal aspects of such a scheme;
 - Compliance with Australian legislation;
 - Complaint procedures for incorrectly classified content;
 - The scope of filtering (to be undertaken in consultation with the *general public*): what is to be filtered; how often is filtering to be applied; how often will filter lists be updated and provided to ISPs; and
 - How will content be classified; what levels of transparency, scalability and security will apply to the classification process.
- Mobile Internet service providers should be included in the consultation and planning activities.

Undertaking these recommended steps would ensure that a detailed set of requirements could be provided to ISPs. Detailed requirements are necessary for any successful implementation of filtering and for proof of concept testing.