

PART 3

INTERNATIONAL SURVEY

**Findings on the Nature and Extent of Options
Employed Elsewhere**

TABLE OF CONTENTS

SECTION A: BACKGROUND AND APPROACH	3
1.0 Project Background.....	4
2.0 Project Objectives	4
2.1 International Survey.....	4
3.0 Approach.....	5
3.1 Factors for consideration during interviews	6
SECTION B: FILTERING OBJECTIVES, LIST MANAGEMENT AND STRATEGIES IN EUROPE	8
1.0 Filtering Objectives in Europe	9
2.0 List Management and Filtering Strategies in Europe	9
2.1 Blocklists.....	9
2.1.1 The Role of Hotlines in Blocklist Creation	10
2.2 Central Filtering Strategy.....	10
SECTION C: COUNTRY PROFILES	12
1.0 European Country Matrix	13
2.0: Detailed Country Reports	14
2.1 Belgium.....	14
2.2 Denmark.....	15
2.3 Finland	16
2.4 Germany.....	18
2.5 Ireland	20
2.6 Italy	21
2.7 Norway.....	23
2.8 Sweden.....	23
2.9 United Kingdom.....	25
3.0 General Observations about Filtering in Europe	26
4.0 Key Findings	27
5.0 Key Issues	28
APPENDIX A: IWF STATEMENT ON URL LISTS	33
APPENDIX B: EXTRACT FROM EU ECOMMERCE DIRECTIVE	36
APPENDIX C: ORGANISATIONS CONTACTED.....	41

SECTION A: BACKGROUND AND APPROACH

1.0 Project Background

The Feasibility Study on ISP Level Filtering was initiated in August 2007. The study was supported by 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 *'Terms of Reference'*) of 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, barriers to industry compliance, policy considerations and international precedents.

2.1 International Survey

This international survey is intended as a component of the broader joint industry/government study that has examined options for ISP content filtering in Australia.

The survey does not consider the merits of the overseas systems that are identified or reflect on their success in filtering Internet content generally. Instead, the survey has been undertaken to better understand the nature and extent of filtering as it occurs elsewhere and to provide some insights into options that might be considered for evaluation as part of the main study.

The purpose of the international survey is primarily to provide information on model options for consideration as part of the broader study. The international survey does not consider all factors within the '*Terms of Reference*' as they apply to each international jurisdiction surveyed. The international survey is itself one element of the '*Terms of Reference*' and is intended to stand on its own. However, where information is available which pertains to the '*Terms of Reference*', these have been noted as observations; for example, in relation to the *Term of Reference* – 'the degree of compliance in jurisdictions surveyed'.

The survey does not recommend specific models for application in Australia.

3.0 Approach

Between September 12 and October 5 2007, 32 organisations (see Appendix C of this survey) were interviewed across 10 jurisdictions in Europe and the USA with the objective of acquiring information on the nature and extent of Internet filtering in each place. Europe, in particular, is the epicentre of regulatory activity in regard to ISP level filtering. Developments in Europe are the most applicable to policy formulation within western democratic contexts, i.e. Australia, and the focus of the survey is very much on Europe. At the time of writing this report there was no ISP level content filtering in the USA.

The jurisdictions were selected on the basis of prior research that indicated those places in which some form of server level filtering is in place. Organisations in the USA with a presence in Europe were visited to validate the European experiences.

As the main study is intended to consider potential options for implementation in Australia, it was agreed that an international survey would assist in the formulation of potential models for Australia.

The jurisdictions to be surveyed were agreed in advance with the Department of Communications, Information Technology and the Arts (now the Department of Broadband, Communications and the Digital Economy).

In conducting the interviews, each representative was asked to provide general background on their respective scheme and to relate experiences on the success or otherwise of the methods being employed.

Where information was not readily obtainable, interviewees agreed to the follow up provision of documentation to augment the content obtained during the interview process. In some cases, additional information was not obtainable and information has been provided from secondary sources, or online. Where this material is included here, its source is stated.

3.1 Factors for consideration during interviews

The following information was sought during the interview process. Not all information was provided by all jurisdictions.

- Nature of the scheme: Is it voluntary or mandatory?
- What law applies?
- Who administers the law?
- What subject matter is subject to filtering? E.g. child abuse images, gambling, other.
- Is there a regulatory authority with jurisdiction to enforce compliance?
- What is the level of compliance with the scheme? Only large players, industry association members, whole industry?
- What is the market size and structure? Roughly how many ISPs in each market? Is there one dominant ISP, market concentration among a few players, widely distributed market share?
- If there is one dominant ISP, are they government owned, and to what share?
- Are they required to take direction from the government generally, e.g. a license condition or by 'persuasion'?
- Who determines the content of relevant blacklists?
- How is the blacklist distributed?
- Is it subject to confidentiality and how is this achieved and maintained?
- How is the blacklist implemented at the ISP level? E.g. What is the process, frequency of updating list etc?
- What technology is involved?
- Do we know the architecture involved? If so, provide details.

- What costs are likely to be involved for the industry or each ISP? If a figure is not available, is the cost likely to be burdensome; substantial but manageable relative to the size of the operation; minimal, such that ISPs of any size can comply?
- Any other considerations relevant to general questions of implementation?

SECTION B: FILTERING OBJECTIVES, LIST MANAGEMENT AND STRATEGIES IN EUROPE

1.0 Filtering Objectives in Europe

The focus of ISP filtering in Europe is primarily on the protection of children through preventing the availability of child abuse images on line.

It is this context in which filtering is carried out internationally. It is recognised that this is only part of a broader approach to addressing the availability and access to child abuse images online. The other components are law enforcement activity, hotlines for the reporting of child abuse images and education programs. Co-regulation often involves a sharing of responsibilities, not always under legislation or even as part of a coherent, integrated scheme. Nevertheless, various elements are pulled together to provide a complementary set of solutions to tackle the problem of the availability of child abuse images online.

2.0 List Management and Filtering Strategies in Europe

2.1 Blocklists

The most common filtering technique in Europe involves using a ‘blocklist’¹ or ‘blacklist’ indicating which content should be blocked. For the purposes of this report the terms blocklist and blacklist are used interchangeably.

Some lists called ‘allow lists’ indicate age-appropriate/work-appropriate content which can be viewed and blocks anything *not* on this allow list.

In some circumstances the ‘blocklist’ is created using the self-determined or third party-determined rating of Internet content. The content is catalogued (called ‘rated’) using guidelines to determine how much nudity, violence, sex or foul language is contained in the content and then the content is blocked by configuring the system to reject specific categories of content.

¹ Blocklist is the term more commonly used in Europe for the URLs of illegal sites. In Australia the term used is Blacklist.

2.1.1 The Role of Hotlines in Blocklist Creation

The INHOPE² International Network of Internet Hotlines, established in November 1999 and funded under the European Community Safer Internet Plan, combats illegal content and activity on the Internet. This fight against illegal content invites Internet users to report illegal content that they accidentally find whilst using the Internet. This very effective process generated over 500,000 reports to INHOPE hotlines during 2005 and 850,000 reports in 2006, with these numbers constantly increasing. Some INHOPE members also deal nationally with other types of content. Over 9600 reports about child pornography are sent to law enforcement every month.

When a hotline receives a report about illegal content, the hotline reviews that content on the Internet and then traces the location of the content. If this trace is outside the hotline's country the report is forwarded to the hotline in the country where the material is located. If there is no hotline in that country the URL is forwarded to the national police, who then add that URL to the blocklist.

A side effect of the hotline approach is that Internet users must sometimes view these images before they are reported to a hotline for processing.

In addition, some users might deliberately try to find such material for personal pleasure even though viewing such images causes ongoing re-victimization of those pictured or filmed.

2.2 Central Filtering Strategy

Central filtering has been used in businesses and schools for many years. These are environments that are easier to control as the complete network is under the control of the IT management team. In a public network there are many different technologies in use that are not always directly under the control of the network operator.

Voluntary central filtering on a public network for the purposes of anti-Spam, anti-phishing and anti-virus protection has increasingly been adopted in recent years as of benefit to customers. This protection option is usually deliberately chosen by the

² ACMA is a member of the International Network of Internet Hotlines since 1999.

customer for specific areas of concern, i.e. different types of malware including virus protection.

Mandatory server-based-filtering on a public network has only recently begun as an offering to customers and society by enforcing certain types of filtering. The primary filtering is performed on child abuse/child pornography images hosted on websites. The types of content that can be filtered are restricted only by the contents of the blocking list, but large scale filtering has only been adopted in a narrow range of democratic countries with limited success. Depending on the system in use, as the size of the blocklists grows, the quality of non-filtered Internet traffic can be compromised.

For detailed information on Filtering Techniques please see Part 2, Appendix K of this report.

SECTION C: COUNTRY PROFILES

This section summarises the main features of ISP filtering for each country surveyed in Europe and provides details on the context in which it occurs.

1.0 European Country Matrix

	Belgium	Denmark	Finland	Germany	Ireland	Italy	Norway	Sweden	UK
Type of Filtering	URL	DNS	DNS	URL	URL		DNS	DNS	URL
Who determines blacklist content?	LEA ³	LEA/ Hotline	LEA	Govt	NGO ⁴	LEA	LEA	LEA/ Hot line	NGO
Is there a central list server?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Is there a central server for filtering? ⁵	No	No	No	No	No	No	No	No	No
Is the message 'Http:404' given to show a blocked site?	No	No	No				No	No	Yes
Is a warning message provided stating that a site is blocked and any other relevant details (if appropriate)?	Yes	Yes	Yes				Yes	Yes	No
Is ISP Filtering mandatory or voluntary?	Voluntary (Only 1 ISP thus far)	Voluntary	Voluntary	Voluntary	Voluntary	Mandatory	Voluntary	Voluntary	Voluntary
What type of material is filtered? ⁶ CP = Child Pornography G = Gambling	CP	CP	CP	CP	CP	CP/G	CP	CP	CP

³ LEA = Law Enforcement Agency

⁴ NGO = Non Government Organisation

⁵ A central list of servers is the single source for providing blacklist URL details.

⁶ The degree of enforcement was not ascertained.

2.0: Detailed Country Reports

Please refer to Appendix B of this survey for the EU eCommerce Directive (Extract) referred to in the country reports below.

2.1 Belgium

In Belgium, reports about illegal content are directed to a hotline. The hotline refers reports to the police, because under Belgian law (as with Norway) it is illegal to view child abuse images.

The hotline attempts to determine the location of the relevant sites. Where it is based within Belgium a takedown notice is issued to the relevant content hosts. Where the site is deemed to be hosted internationally, it is referred to INHOPE.

There is a non-binding protocol between ISPs and police that was established approximately two years ago. DNS poisoning is being explored as an option here, however there is neither a formalised blacklist nor a process by which one could be created. Were one to emerge, it would probably be provided by police, given that they would have law enforcement justification to view sites which could be subject to ISP filtering.

Only one Belgian ISP (Scarlet) is currently filtering content, and this is done voluntarily. They obtain information from the Dutch KLPD (Korps Landelijke Politiediensten) who provide them a list of IP addresses and URLs to which access is blocked. This list is confined to CP images, is shared internationally, and is updated by Law Enforcement Agencies (LEAs) from other countries on a regular basis. Scarlet customers who try to access one of the sites on the list are served with a page that tells them the site is not available because of the content contained on it.

At the time of producing this report the Belgium was experiencing an interregnum in government. The result being that there was no mechanism for the passage of new laws. Therefore, even if a requirement to filter was mandated, and there is no suggestion that this is planned, no legislative obligations upon ISPs will take place within the foreseeable future.

2.2 Denmark

Denmark passed domestic legislation in 2002 to transcribe the EU eCommerce Directive 2000.

An ISP Forum was established in 2002, which is a joint group involving industry, regulatory authorities and NGOs. The ISP Forum exists as a practical means of assisting with the implementation of the law as it pertains to ISPs.

For example, Article 14 of the Directive gives no guidance on how to implement, and therefore the ISP Forum has been considering proactive measures that ISPs can take as a defence against further legislation.

The industry was initially opposed to ISP level filtering but has conceded in relation to child abuse images. Currently filtering is performed at the ISP end, although participation is voluntary and doesn't span the entire industry.

In terms of market share, the main players are TDC, Telia and Cybercity, which collectively cover approximately 90% of the market.

The rest of the industry comprises 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. These smaller businesses are not members of the ISP Forum either.

In summary, ISP level filtering of child abuse images remains as a voluntary scheme, though there is concern it could become mandatory, and could be expanded to include other kinds of content. However the Danish constitution contains guaranteed rights to free speech and serves as a check on legislatures.

The list that ISPs are using is developed combining reports to a local hotline with the IWF list. These are consolidated by the Danish police and provided to participating ISPs. There is no prescribed frequency for refreshing the list (as there is in Italy). ISPs are at liberty to implement internally as they see fit. Filtering occurs at the DNS level, not at the IP Level.

In Denmark, possession of child abuse images is illegal but there is no distinction made in blocking sites that are commercial as opposed to non-commercial, as there is in Sweden.

2.3 Finland

There is a very extensive debate in Finland on web blocking under Finnish legislation and especially concerning the ‘law of measures to prevent spreading of child pornography’. Previously, there had been uncertainty on the legality regarding whether police had a right to convey the list of web sites containing child pornography to network and service operators. The purpose of enacting this law was to clarify the situation, and to formally legalize the current practice. The act allows the ISPs to block sites and will allow the police to maintain a list of sites.

As a consequence, the Parliament of Finland approved a 2006 Bill without amendment and the law came into force on 1st of January 2007 as the *Communications Market Act 2006*.

Paragraph 2 of the Act defines the ‘Network operator’ and ‘Service operator’, to whom the law will be applied:

This particular paragraph refers to definitions in the Act and there are the relevant definitions. According to the Act: a network operator means an operator that provides a communications network in its ownership or for other reasons in its possession for the purposes of transmitting, distributing or providing messages; and service operator means an operator that transmits messages over a communications network in its possession or obtained for use from a network operator or distributes or provides messages in a mass communications network.

The Ministry of Communication has indicated that the law merely serves to legitimise an existing practice, the legality of which had been questioned by ISPs.

A voluntary program that Finnish ISPs implemented to curb access to foreign web pages containing child pornography has been in place since September 2005. The Finnish constitution makes it very difficult to pass a law sanctioning *ex ante* censorship of web pages. As a consequence, the intent of the Communication Ministry has always been framed in terms of a voluntary scheme of industry self-regulation,

instead of mandatory regulation. The law therefore breaks new ground and it is likely it will be challenged in court.

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

The Ministry agrees that the system cannot 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. The Minister of Communications accepts that the system will not stop most persons who intentionally attempt to access child pornography pages. The point is, however, that the system *will* prevent Internet users from accidentally accessing pages that containing child pornography.

Currently there is no official list supplied. ISPs do, however, receive notifications from an organisation called 'Rädda Barnen' ('Save the Children') in Sweden that are then transferred to the police for confirmation.

The Ministry of Communications states that the full official list (of sites containing child pornographic material) created by police would be ready by the end of 2007⁷.

An MoU between the National Bureau of Investigation and FiCom (the Finnish communications industry association) is also proposed. This will enable police to provide a list by email to all operators who will voluntarily filter. ISPs would prefer to be able to poll the list remotely via a secure site.

ISPs are looking at nominating a role rather than a person as the contact point, to give flexibility for leave arrangements and other availability issues.

In summary, the current scheme in Finland remains voluntary. There is no legal obligation for ISPs to block sites, nor is there any agreed method of implementation. Nevertheless, at the time the interviews were held in Finland, the target was that by the end of 2007 every main operator would be blocking child abuse images⁸. As to the

⁷ An update on the status of this official list was requested form Ficom but was not available at the time of writing this report.

⁸ IBID

smaller providers, it will be up to the police to encourage compliance. FiCom is encouraging its own members to comply.

This is being done in the hope of reducing the need for legislation. Industry also wishes to demonstrate a responsible approach to this issue.

Due to the newness of the proposals, the law is not yet fully implemented, as ISPs and government work out some technical aspects in terms of provision of a list. They are considering using ICAP – ‘Internet content access protocol’. Blocking is being done using BGP – ‘Border Gateway Protocol’ – at the IP level.

In relation to DNS blocking, the ISPs are provided with a list of URLs. The user is redirected to an information page, stating to the effect ‘your browser has attempted to contact a page which includes illegal material. If you have reason to believe you have been wrongly directed, please send an email to the police’.

Currently the list is encrypted using PGP. An ISP must provide two contact names, one technical and one administrative. The PGP keys are provided to these two nominees.

The Finns are concerned about scope creep. While there is a constitutionally guaranteed right to free speech, the degree of industry support for extended measures remains problematic - as it does in the rest of Europe.

2.4 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. There is significant pressure particularly in relation to hate speech and Nazi sites.

Most German ISPs implement filtering using DNS poisoning. This is in response, in part, to research pointing to vulnerabilities in a Cleanfeed style approach.⁹

A comment provided by one industry representative is as follows:

The German eCommerce Association is critical of British BT Cleanfeed filtering system due to its lack of transparency (IP

⁹ For example: ‘Failures in a Hybrid Content Blocking System’ by Dr Richard Clayton, <http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf>.

filtering, 404 error) and publicly accountable procedures. They refer to examples such as in Denmark where 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.

In Germany, the industry and government seek to distinguish between illegal sites and those that would be restricted (e.g. mere adult sites) which could be limited by age verification.

In implementing the EC eCommerce Directive, Germany has applied the following principles:

- The content provider is primarily liable for content
- The content host must respond to a take down notice
- A mere conduit is immunised against liability, however is still subject to the General Law.

The courts have applied this to require ISPs to undertake selective blocking in cases where there is no disproportionate damage to their business, either technically or on a cost basis, where the ISP is a willing participant in the breaking of the law and where they have the ability to stop their participation, even if stopping it will not stop the conduct.

These general principles have been outlined in obiter decisions (of German courts) to potentially apply to copyright, trademarks and other matters. The qualifier seems to be that the number of sites in question is small - hence manual blocking is feasible; large numbers of sites would fail the proportionality test.

However, these days it is arguable that, with automation, the number of sites that could be ordered down could be increased without offending the proportionality principle.

The Germans observe that in Norway a constant feature of HTTP requests is that they have remained fairly static in number, e.g. around 70,000 per month. There are three possible reasons for this. Firstly, there could be the same number of people attempting to access the sites every month, to see if they are still there. Secondly, they are different people, however, it is questionable that exactly same number of people

looks at the content. Thirdly, and more probably, the constancy of traffic is suggestive of automatic polling by bots and search engines. It is noted that in Norway, mere viewing of child abuse images is illegal.

As in Sweden, industry here has concerns about the interpretation of the high volume of HTTP requests to blacklisted sites. This implies a high number of offenders in the jurisdiction, whereas the general view is that these figures exaggerate the demand for access to illegal sites. This has tempered the appetite for greater industry pro-activity in restricting access as have other countries.

It should be noted that the German system of search filtering is in place, and is seen to have advantages in being more transparent to users. The list emanates from KJM, which is accountable as a public authority (as opposed to IWF, which, as has been observed elsewhere in this document, has had its legitimacy questioned in other EU jurisdictions). 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.

2.5 Ireland

Under the *eCommerce Act 2000* which transcribed the EU eCommerce Directive into Irish law, Irish ISPs must act in reasonable time to remove illegal content of which they have been given knowledge from public access on systems under their control. 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 this jurisdiction.

The industry has largely been given the right to self-regulate in the area of child protection generally. See for example the 2005 parliamentary debate on child sex offences.¹⁰

The Irish industry is not averse, in principle, to the protection of customers through filtering but believes it needs a proper framework in which to operate.

Presently the *Child Trafficking and Pornography Act 1998 to 2005* imposes no obligations on ISPs to filter content. It does however criminalise the possession of and dealing in child abuse images.

¹⁰ <http://historical-debates.oireachtas.ie/D/0601/D.0601.200505050156.html>

The official position of the Association (ISPAI) in relation to blocking child abuse images is as follows:

In principle the ISPAI supports exclusion of such web content from customer access, subject to legally binding assurances from government or legislation to approve actions necessary for its achievement, member organisations are unable to propose a single policy or solution that is appropriate across all sections of the ISP industry.

There is little support for BT-style Cleanfeed system, due to issues of legal liability for ISPs. The issue remains controversial and no uniform view has yet emerged.

2.6 Italy

Pursuant to Italian Law Number 38, which came into effect on 6 February 2006, Internet Service Providers must have processes in place to deal with access to child pornography.

Specifically, ISPs are required to have in place filtering mechanisms to prevent access to proscribed sites as advised by a special centre dealing with such activities – the CNCPO (Centro Nazionale per il Contrasto della Pedopornografia sulla rete Internet).

By way of Decree issued on 8 January 2007 by the Ministry of Telecommunications, ISPs are responsible for reporting to CNCPO with a specific implementation plan in line with the guidelines listed below.

Each ISP will be required to submit a filtering plan within 15 days upon advice from the Ministry.

Additional requirements for ISP's are as follows:

1. Required filtering will be mandatory at least at FQDN level (Fully Qualified Domain Name) for all sites which will be declared forbidden by CNCPO, or also at 'IP address' level where specifically required.
2. Websites to be made forbidden will need to be forwarded to a specific web page each ISP must build (contents/shapes to be received by CNCPO).

3. Websites to be made forbidden will come from a list (with related URL) contained in a specific 'Ministry web page' (no information available yet) from which downloads will be made possible
4. The list composition may be different (sites listed per URL, per IP address, per domain), but in any case, there will be a code per list item (dd/mm/yyyy format) at the beginning of the file.
5. New lists to be downloaded may contain either new entries to be blocked, or those to be restored (where, for example a URL has changed).
6. The list must be downloaded at least once a day (10:00am), weekends possibly included, but only if specifically asked.
7. The list must be implemented into each ISP's IP network:
 - By 16:00hrs in case of site inhibition task
 - By 22:00hrs in case of site reinstatement task
8. Secure HTTP protocol is specified to access the Ministry web page, and download processes will be done via SSL certificates provided by the Ministry.
 - Lists will be acquired via GET commands applied on URL, such as:
 - `https://<host>:<port>/<Denied_FQDN_list>`
 - `https://<host>:<port>/<Denied_IP>`
 - As a result of above operations, a 'csv' file will be obtained, with a progressive number allowing ISPs to determine if a given list is the one with the latest instructions to be implemented.
9. Each ISP is required to provide CNCPO with feedback on instances of inhibition/reinstatement via encrypted mail (digital certificates to be provided by them). This message body should include list ID, time, date, and type of intervention made. Communication via fax is allowed only in cases of mail service unavailability.
10. The Ministry should be made aware of a fixed IP address for a specified PC designated within each ISP for the purpose of downloading the blacklist.

11. The Ministry is required to be advised of a specific fax number, a specific SMTP address to send/receive mails, a specific list of entitled names to manage all above communications.

2.7 Norway

In Norway, police provide a blocklist to ISPs who must then remove content or block access depending on whether they are hosting content or simply providing network access.

There are about 50 ISPs in Norway. Telenor, the largest operator, which is 90% government owned, has offered to assist police in filtering child abuse images, similar to BT in the UK, and has decided to make it cross-industry.

There is a standardised agreement between Telenor and the police. The model is different from Cleanfeed, where a '404' error message is presented. In the Telenor case, users are redirected to an actual message from the police, which is considered to be more transparent.

Sweden and Denmark have both implemented similar systems.

There is no compliance monitoring in relation to filtering in Norway. Consistent with other European jurisdictions, it is up to each ISP to determine how they wish to block access, i.e. ISPs can implement as they see fit. Based on interviews conducted it is understood that DNS filtering is the preferred option amongst ISPs.

In Norway, filtering remains a voluntary system and there is no sanction for non-compliance. However in Norway, it is unlawful to view child abuse images.

By agreement with police there is also no logging of traffic. Instead, the police are using international payment systems to investigate crimes relating to the depiction of child abuse.

2.8 Sweden

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

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

Under a written agreement between the police and each participating ISP, the police define and list which sites that fall within the parameters of commercial child pornography according to Swedish law.

ISPs, for the purpose of the agreement, are Internet *access* providers (as opposed to search or online content providers), who are participating in the scheme.

In Sweden, all major ISPs are participating in these voluntary arrangements. This includes Com Hem, TDC Song, Tele2, TeliaSonera, Telenor and 3. Collectively they cover over 80% of consumer access customers.

The ISPs provide feedback on the scheme by providing anonymous statistical information on server requests to the police. Currently these number about 30,000 per day.

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 the financial incentive for commercialising child abuse images.

The parties acknowledge that the scheme is not 100% effective. It is dependent on the extent of the list; sites that are identified are not taken down, as they are usually

outside of jurisdiction; and it does not render access via proxy or other ISPs impossible.

For these reasons, effectiveness at large is difficult to judge. The number of the pages blocked and searches per day are known, but facts on the actual results, that is to say, the proportion of child pornography sites caught by the scheme, is not known.

2.9 United Kingdom

It is now well known that British Telecom (BT) introduced Cleanfeed in June 2004. The reasons for its introduction and the manner in which it was done remain the subject of some controversy in Europe.

Under pre-existing arrangements in place since 1999, Internet users who believe they have found a site containing child abuse images are encouraged to report the site to the Internet Watch Foundation (IWF), via its website or by a telephone hotline.

IWF analysts trained by the National Crime Squad review the reported sites for evidence of illegal material. Locally hosted sites are addressed via a notice and a takedown regime administered by the IWF.

Sites that are not subject to takedown, due to hosting offshore, are added to the IWF blacklist, which is then provided on a confidential basis to participating ISPs.

A description by IWF on the manner in which URLs are determined is provided below:

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.

BT Cleanfeed at present filters approx 1800 URLs but the maximum number of URL's it is thought to be able to filter is thought to be into the 100s of 1000s¹¹. BT has disclosed that its servers block 35,000 daily attempts to view child pornography. However this figure has been queried on the basis that the metric referred to was

¹¹ This information was provided by Nick Truman – Head of Internet Security at BT Retail, in Feb 2008.

'hits', which can exaggerate the demand for content. See, for example, these comments from the Internet Service Providers Association:

[The] ISPA feels caution is needed with the information and statistics so far available on Cleanfeed. It is very difficult to comment on the statistics reported by BT regarding Cleanfeed as BT has not passed the data to ISPA. At present there seems to be a significant disparity in the statistics that are being reported.

BT has provided an estimate cost for implementing the ISP level filtering of child pornography at a retail level (not wholesale level), within the BT network environment, of £500K¹².

3.0 General Observations about Filtering in Europe

3.1 Industry Compliance

The focus in Europe is very much on the protection of children through the blocking of child abuse images.

In none of the 10 jurisdictions surveyed is there a legal obligation on ISPs to block or filter child abuse images (CAI).

In Scandinavian jurisdictions, the extent of voluntary compliance appears to be very much tied to the dual factors of market structure and extent of government ownership of ISPs.

For example in Norway, Telenor has the major market share and is almost fully government owned and controlled. To the extent that it has voluntarily adopted DNS filtering of child abuse images, it follows that the majority of Internet users will receive a filtered service.

¹² IBID

In Denmark, the majority market provision is split between three major players: TDC, Telia and Cybercity, which collectively account for 90% of the market. These players are voluntarily blocking CAI.

The residual are not thought to be adopting such measures. This is consistent with exemptions provided to them under legislation relating to the logging of usage pursuant to anti-terrorist legislation (introduced in 2004 and emended in 2007).

The situation is substantially different in Sweden and Finland however, where the industry is highly disaggregated and where, as a result, voluntary compliance is thought to be somewhat less.

4.0 Key Findings

- *Approach*

Respondents generally agreed that the ideal method of preventing child pornography on the Internet is to have them removed by the hosting provider and by prosecuting the producer of the images so that the child can be protected from further abuse.

- *Role of Legislation in Prevention*

Most Internet child pornography is hosted in countries and by Internet access/hosting providers where national legislation is not comparable to best international practice and standards, and where notice-and-takedown procedures do not work correctly.

- *What is Achievable*

Filtering does not prevent the production of child pornography but it does make it more difficult to access this content so that only more determined and technically skilled Internet users will be able to access it. It can also disrupt the revenue stream for commercial illegal websites.

- *Protection of Free Speech*

Many jurisdictions surveyed have constitutionally protected free speech that creates limitations on the extent of content filtered, specifically on the range of content which

can be filtered. In some cases, such as in the US, laws that originally sought to impose obligations on ISPs to filter content have been overturned. In jurisdictions where industry has agreed to filter voluntarily, it has been done either as a commitment to good corporate citizenship, or under threat of regulation.

- *EU Directive*

The Directive 2000/31/EC of the European Parliament and of the council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) is the key EC legislation moulding the response of European governments to Internet filtering in European countries.

This directive is responsible for defining the level of liability of Internet Service Providers in relation to illegal content on the Internet and is the underlying legal cornerstone for the effectiveness for the EU-funded hotline network – INHOPE. According to this instrument, 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. via a hotline).

5.0 Key Issues

- *Legal Constraints of Filtering*

Within the jurisdictions interviewed filtering has been criticised for being in contradiction to the principles of freedom of expression and/or for being technically inaccurate (e.g. over-blocking of sites where IP or whole domain addresses are blocked) but this depends on the range of content being filtered and how large this range is.

- *Scope Creep*

In all jurisdictions surveyed, industry respondents raised the issue of scope creep or the ‘slippery slope’ as a real barrier to embracing more proactive measures to limit access to child abuse images.

The concern is that the introduction of mandatory Internet filtering at the ISP level for the purposes of limiting access to child abuse images will pave the way for a host of other sites to be blocked, ranging from other criminal areas through to civil actions relating to defamation and copyright.

It was repeatedly expressed in interviews that the willingness to engage in responsible cooperation with law enforcement agencies in relation to child abuse images would be tested should the extent of what is being blocked be seen to gradually expand.

- *Compliance with Legislation*

In the EU, compliance with blocking remains voluntary, with the exception of Italy in relation to child pornography and gambling sites.

Compliance by industry, which is at best patchy, is nevertheless predicated on the assumption that it is only child abuse images that will be blocked.

Levels of compliance are largely tied to organisational size. This is usually a corporate decision based on the perception of social responsibility, and the fact that, as larger ‘targets’, market leaders believe they cannot afford to be seen to be resisting conformity with social norms in relation to child abuse images – for which there is general community abhorrence consistent across jurisdictions. This is reflected in laws that make the dealing of and in most cases, possession of child abuse images a criminal offence.

However, progression down the ‘food chain’ of ISPs yields a lower level of compliance. A number of factors are likely to be at play here. On the one hand, small ISPs were established during a time when computer bulletin boards ‘morphed’ into commercial ISP operations. Telecommunications deregulation in most jurisdictions

has resulted in the ability of just about anybody to commerce in ISP operations without license. The same is true in Australia.

Many smaller ISPs may feel they are less of a target for publicity should they fail to block content. With smaller customer bases, the probability of exposure is notably lower.

In the case of the UK and Cleanfeed, compliance is dealt with by upstream providers.

There is presently no legal obligation on ISPs (other than in relation to gambling sites in Italy) to filter or block child abuse images, therefore ISPs are acting within the law by not blocking. There is no question that relations between ISPs and LEAs would be put under pressure should ISPs perceive that child abuse images filtering was the ‘thin end of the wedge’ for an expansion of materials to be blocked. This will form a material consideration in any Australian implementation of a mandated filtering requirement.

It should be added however that in the Scandinavian jurisdictions free speech is constitutionally protected, and those interviewed believe that pressures on industry to filter broader categories of content will be constrained by these limitations on legislatures. See the below extracts from the EU eCommerce Directive, Article 14 and Article 15, which also serve to delimit ISP responsibilities.

- ***List formation***

There is no consistent view on which entity is best placed to develop blocklists/blacklists. Largely, the view is a function of culture and historical precedent.

In the US, for example, there is a strong view (based on First Amendment principles) that it is not the role of government to determine what content citizens may view.

There, companies – where they believe they have any role to play in limiting access to

CAI – believe that privately developed lists (e.g. from the National Centre for Missing and Exploited Children) are the preferred source of list material.

In the UK, the Internet Watch Foundation (IWF) is a privately run organisation that has legal recognition for its role in ascertaining CAI and sites to be blocked. While this has the general support of industry in the UK, it cannot be said that the IWF list is supported throughout the rest of Europe. Generally, concerns were raised about the IWF process on two counts.

Firstly, the lack of transparency in list preparation; and secondly, the right of a private organisation that is member-funded to provide lists only to those who fund it. In combination, these two factors give rise to a general view outside the UK that questions the legitimacy of the IWA list process. While there are moves to have the IWF list recognised as a standard throughout Europe, it is not likely that this will emerge in the foreseeable future.

In other jurisdictions where there is a greater cultural trust of government (notably the Scandinavian countries), ISPs had no difficulty with the concept of police being the appropriate bodies to consolidate lists and provide them to ISPs. This is in fact the case in all Scandinavian jurisdictions as well as Italy.

Interestingly, Australia's process of an independent statutory authority (ACMA) as the list originator met with a range of responses, from support, on the one hand, for the fact that ISPs did not have to make the call on the legality of content, to consternation on the other, in jurisdictions where the right of government to determine what people should see is considered anti-democratic.

- *Security of blocklists*

During interviews in some jurisdictions, concerns were expressed as to the security of blocklists and the liability for ISPs should blocklists fall into criminal hands.

Solutions under consideration include legal indemnities for ISPs who are acting in compliance with lawful requests to exercise reasonable efforts to block content. In places such as Norway and Italy, the industry is pressing for secure web access that will permit the automatic polling of an online resource to reduce human intervention. A hash file system will flag whether the list has changed and will assist in the automation of the process. This option is being pursued from a cost standpoint and also a security one, where ISPs fear for liability should a list within their possession, custody or control be misused.

APPENDIX A: IWF STATEMENT ON URL LISTS

Child Sexual Abuse Content URL List

www.iwf.org.uk

The diversity and quality of the services we provide to our members continues to increase. Our child sexual abuse content service developed as an industry-led initiative has gathered pace since 2004.

As a result of work by our analysts, potentially illegal URLs are regularly added to our unique list of online child abuse content. This list is dynamic and comprehensive: updated twice a day. The *Protection of Children Act 1978* as amended in the *Sexual Offences Act 2003*, makes it an offence to take, make, permit to be taken, distribute, show, possess with intent to distribute, and advertise indecent photographs or pseudo-photographs of children under the age of 18. The ‘making’ of such images includes downloading, that is, making a copy of a child abuse image on a computer, so, in the UK, accessing such content online is a serious criminal offence.

Despite success in almost eradicating this content from UK networks, sexually abusive images of children are still available around the world, so the commitment by our members to voluntarily prevent the accidental download of such content by working to deploy our list on their services has been welcomed in many quarters. Since 2004, many more of our members have chosen to make use of this service, namely, Internet service providers, mobile operators, search providers and filtering companies. Law Enforcement Agencies and associated Hotlines who are members of INHOPE can also choose to have access to the list. [**Authors Note:** This would also permit ACMA access to the IWF list.]

This list typically contains between 800 and 1200 live child abuse URLs at any one time. As the URLs are precise websites or web pages the risk of over blocking or collateral damage is minimised.

As a result of this initiative it is possible to:

- 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.
- Disrupt the accessibility and supply of such content to those who may seek out such images.

Unfortunately, the blocking mechanism cannot put an end to offenders abusing children or distributing images of child sexual abuse on the Internet but at least this initiative contributes to an overall solution.

Our systems and processes in compiling this list have been inspected and validated by two eminent professionals and found to be consistent with best practice. There is a procedure whereby the website owner of any blocked URL has the right of appeal. The URLs are assessed according to UK law, an expert process reinforced by reciprocal police training with each image being categorised in line with criteria set out by the UK Sentencing Advisory Council. Details of every URL with child sexual abuse content are passed with accompanying intelligence to our partners at the Child Exploitation and Online Protection Centre as well as our Hotline associates around the world.

Blocking facilitated by the use of our list applies only to website content. We have no role or remit for tackling the distribution of child sexual abuse content through other channels such as peer-to-peer or instant messaging.

**APPENDIX B: EXTRACT FROM EU ECOMMERCE
DIRECTIVE**

The following is an extract from the EU eCommerce Directive. Specifically;
Section 4 of that Directive - Liability of intermediary service providers

Article 12

"Mere conduit"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that *the service provider is not liable for the information transmitted*, on condition that the provider:
 - (a) does not initiate the transmission;
 - (b) does not select the receiver of the transmission; and
 - (c) does not select or modify the information contained in the transmission.
2. The acts of transmission and of provision of access referred to in paragraph 1 *include the automatic, intermediate and transient storage of the information transmitted* in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.
3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 13

"Caching"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that *the service provider is not liable for the automatic, intermediate and temporary storage of that information*, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:
 - (a) the provider does not modify the information;
 - (b) the provider complies with conditions on access to the information;
 - (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
 - (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
 - (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 14

“Hosting”

1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
 - (a) *the provider does not have actual knowledge of illegal activity* or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
 - (b) *the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.*
2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.
3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

Article 15**“No general obligation to monitor”**

1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, *nor a general obligation actively to seek facts or circumstances indicating illegal activity.*

 2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.
-

APPENDIX C: - ORGANISATIONS CONTACTED

International Organisations

(Yellow = Regulatory Organisation, Light Green = ISP/ ISP national representative body)

	Organisation	Country
1	UK ISPA	UK
2	Yahoo!	UK & Ireland
3	British Telecom	UK
4	Internet Watch Foundation	UK
5	INHOPE (International Association of Internet Hotlines)	Ireland
6	ISPAI	Ireland
7	Associazione Italiana Internet Providers (AIIP)	Italy
8	Vodafone	Europe
9	Verizon Italia	Italy
10	Freiwillige Selbstkontrolle Multimedia-Diensteanbieter	Germany
11	ECO Verband der deutschen Internetwirtschaft	Germany
12	FiCom (Finnish Federation for Communications and Teleinformatics)	Finland
13	Rognlien Djonne Galtung Gardarsson	Norway
14	IKT Norge	Norway
15	Medietilsynet (Norwegian Media Authority)	Norway
16	Medieradet (Swedish Media Council)	Sweden
17	TeliaSonera	Sweden
18	Verizon Business Scandinavia	Norway/Sweden/ Denmark/Finland
19	Save the Children	Denmark
20	TDC	Denmark
21	EuroISPA	Belgium
22	Liberty Global	Netherlands
23	Internet Service Provider Association	Belgium
24	Facebook	USA (in London)
25	Facebook	USA (in New York)
26	Yahoo!	USA (in Washington)
27	USIIA	USA
28	AT&T	USA
29	Verizon	USA

	Organisation	Country
30	Universal Service Access Corporation	USA
31	Business for Social Responsibility	USA
32	Google	USA