Confidential
Version 22 Nov 2006

Issues associated with possible ISP blocking of illegal child pornography web-sites

Part - 1 Introduction

1.1 Reason for this document

This document is the ISPAI response to the request made by Minister for Children, Brian Lenihan, T.D., at the meeting held with the Association on 27th April 2006, to provide for consideration by his Department, an information paper providing details of the objectives and issues associated with possible ISP blocking of illegal child pornography (CP) web-sites on the Internet hosted in foreign jurisdictions that do not react to requests for their removal.

1.2 No single approach viable for all ISPs

Blocking of CP is a complex subject where diverse views on efficacy exist and an ISP's ability to implement without unacceptable degradation of service is dependent on their equipment, network topology and position in the supply chain.

Hence, while the ISPAI has gone on record stating that "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.

However, as is shown in this paper, various technological implementations are possible that collectively can provide for general exclusion of known CP web-sites from end-user customer access.

1.3 Informational status of this paper

Due to the above, this document is an informational paper. **Please note: this is not an ISPAI position paper.** That is, it does not represent a common ISPAI policy on CP blocking which is collectively agreed by ISPAI member organisations.

This is an information paper to assist government and industry develop a practical framework, in which proactive measures to exclude identified CP URLs from access by end-user customers, can be agreed and safely adopted with confidence by the industry. Such an initiative does not replace but rather complements the reactive (Hotline) measures already undertaken on a daily basis by the ISPAI on behalf of its members.

Issues associated with possible ISP blocking of illegal child pornography web-sites

Part - 2 Summary

Background to problem. The Internet is overwhelmingly a positive global resource. A tiny proportion of that resource is being used for criminal purposes. One such criminal use is the distribution of child pornography (CP).

Current reactive response. ISPAI members in Ireland, along with counterparts in 25 countries have established a network of Hotlines coordinated by the INHOPE organisation, to rapidly act against CP on the Internet. Hotlines respond to public reports of suspected CP, by verifying that the content is illegal, tracing the source and then notifying law enforcement and Internet Service Providers (ISPs) to have it removed from the Internet. Where the source is a country that does not have an INHOPE hotline, the report is passed to law enforcement for transmission to the source country via Interpol.

Limitation of current response. The above system works well and rapidly in countries having an INHOPE Hotline but a loophole exists due to countries existing outside the system that do not react, or react very slowly, to notification of CP web-sites in their jurisdiction. There are some key countries where large amounts of known CP are continuously accessible and can be encountered by Internet users world-wide, including Irish users.

Possible complementary proactive response. In principle ISPAI members support the introduction of means to exclude CP content from customer access, particularly to protect children using the Internet. Technologies, based on block-lists (sometimes referred to as "blacklists") of known illegal sites, have recently been developed whereby known web-sites in foreign jurisdictions can be excluded from access (blocked) without significantly reducing throughput of the Internet. Some ISPs who offer managed Internet services, where customer expectation is for limited Internet access, favour an allow-list (sometimes referred to as "white-list") system, that blocks everything except specified web-sites. "Allow-list" systems are not an option for general Internet service provision to the public.

Issues raised by proactive response. However, the actions required of ISPs in blocking implementation raise many legal, technical and resources issues that must be resolved with government. Some may require legislative changes. Without legally binding assurances on these issues most ISPs feel unable to progress to implementation for fear of criminal prosecution or civil litigation.

Summary of issues. The following is a summary of the issues raised by ISPAI members and the www.hotline.ie service management. These are provided in more detail with explanatory comment in the following sections and appendices.

1. **ISPs placed in role of censor or court of law.** ISPs are not in a position (nor have legal authority) to decide which content residing outside their own servers may or may not be viewed by the citizens of Ireland. ISPs are required by law to remove illegal content from their servers within a reasonable time when notified of its existence and do so at present. (ISPs have right to remove content from their own servers which they deem contrary to their terms and conditions of use as described in their contract with their customers). ISPs should not adopt or be forced to adopt the role of media censors or to be placed in positions of judgment that rightly belong within a court of law.

2. **Control of scope of blocking allowed.** Blocking of CP (to which few would object) sets a precedent for the blocking of other forms of content. In areas other than CP this

impinges on the rights to freedom of thought and expression. ISPs are concerned that if the scope is not set by legislation, pressure groups will seek blocking of content in various areas they claim to be illegal or likely to incite illegal acts.

3. **Questions of legality of actions required to achieve blocking raised by current law.** It is unclear to ISPs whether actions necessary to achieve blocking are illegal under existing legislation. These relate to:

   a. Is the URL of a child pornography web-site, being a means whereby a person using the Internet is directly linked to and shown child pornography, deemed in itself to be an advertisement of child pornography and therefore illegal to possess or distribute under section 5(1)(c) and 5(1)(d) of the Child Trafficking and Pornography Act (1998 to 2005)?

   b. A list of such URLs is required to implement their blocking. If the most expeditious way of blocking the maximum number of illegal sites is to import such a list, does this constitute a breach of the Child Trafficking and Pornography Act (1998 to 2005)?

   c. If the ISPAI Hotline is to receive such a list and add further URLs of which it has obtained knowledge and then distributes this amended list to ISPs, would these activities constitute a breach of the Child Trafficking and Pornography Act (1998 to 2005)?

   d. Would the importation, distribution and hosting, by ISPs, of address information (URLs) pertaining to known illegal child pornography web sites, necessary to achieve their blocking, come under the exception in Clause 6(2)(b) of the Child Trafficking and Pornography Act (1998 to 2005).

4. **Protection of Hotline and ISPs undertaking blocking activity.** The Directors, management and employees of the Hotline and ISPs require either protection in legislation or written legally binding documented assurances from Government, that all actions legitimately carried out in the course of duties as required to achieve blocking, are exempt from prosecution under the Child Trafficking and Pornography Act (1998 to 2005) and other laws that may apply or be enacted.

5. **Employer protection for employees adversely affected.** The Directors and management of the Hotline and ISPs require exemption from civil litigation for requesting employees (under appropriate notification and procedures) to carry out duties required to achieve and maintain blocking, that may involve those employees coming into contact with content deemed to be illegal under the Child Trafficking and Pornography Act (1998 to 2005) and other laws that may apply or be enacted.

6. **Protection from public litigation for unblocked sites or blocking errors.** The Directors and management of the Hotline and ISPs require exemption from civil litigation for any under-blocking (CP sites not being blocked) resulting in customers encountering CP on the Internet or over-blocking (non-CP sites being blocked), that may inadvertently occur from time to time.

7. **Protection for security mishaps.** The Directors and Management of ISPs and the Hotline require exemption from litigation or prosecution where a breach of security occurs that results in possible disclosure of URLs on the block-list unless there is a case of intentional misconduct on their part.

8. **Erosion of "Mere Conduit" status.** Legally binding assurance or a section in legislation must be given to ISPs by government that blocking of child pornography can not be used subsequently as precedent that diminishes "mere conduit" status of

ISPs and telecommunications providers, as provided for under the e-Commerce Directive.

Blocking activities require exemption from litigation. In general, ISPs and the Hotline can not undertake any activities to implement blocking until such time as the government provides legally binding assurances, or legislation is enacted, giving specific exemption to allow these activities to be undertaken without fear of criminal prosecution or civil litigation.

Caution on inward business investment. If legislation requiring blocking of CP were to be enacted without technical exceptions, efficiency of international data transit through Ireland and other international Internet based services could be severely affected, possibly to a level where such carriers or providers would be forced to relocate. It is proposed that any legislation should only refer to retail supply of Internet access services. That is, where the intention is the supply of Internet connection to an end-user customer.

Avoidance of market distortion. In the interests of competition and avoidance of market distortion, any legislation or statutory instrument that would mandate CP blocking must be issued to all ISPs offering retail provision of IP connections. (That is the customer is not themselves reselling, whether or not for reward, IP connectivity outside of their home or organisation. If they are reselling, they constitute an ISP and must be subject to the same legislation or statutory instrument to provide blocking.)

Assistance for small ISP implementation. There is not a "one size fits all" solution to blocking. Some ISPs will require more time than others to achieve implementation. ISPs are concerned that if legislation was enacted requiring immediate introduction of CP blocking by all, smaller ISPs could not sustain the cost and deter new start-up ISPs enterprise. Many such ISPs are providing broadband in areas not served by larger suppliers or they offer the only competition to a major supplier in many locations. It is proposed that some form of relief may be available from government to assist smaller ISPs achieve blocking and allow for a staged implementation up to a certain date.

Issues associated with possible ISP blocking of illegal child pornography web-sites

Part - 3 Detailed discussion

3.1 Background

The Internet provides unbounded access to information on every subject imaginable, entertainment, business and social communication facilities. The vastly overwhelming number of businesses and individual users utilise these facilities for positive and beneficial purposes. Unfortunately a small number of people world-wide use these facilities for improper and sometimes criminal purposes.

Of particular abhorrence to the public, is the clandestine use of the Internet for the distribution of child pornography (CP). ISPAI members have been adamant to act against this misuse of the Internet. In 1999 this action was stepped up when, in agreement with government, the ISPAI established the www.hotline.ie service. This was in line with similar actions in many developed countries where Hotlines cooperate to notify ISPs and law enforcement, so that CP found to be hosted in their countries can be rapidly removed from public access and criminal investigations initiated.

While this approach has been successful in cooperating countries, there are a considerable number of jurisdictions where, even on receipt of notification through appropriate channels, action to remove CP content is either very slow or non-existent. Therefore CP hosted in those jurisdictions remains accessible to Internet users around the world, including those in Ireland. There have been calls from public representatives, child welfare organisations, etc., across the EU for ISPs to block persisting CP sites from access by users. This view has gathered much popular support in the last year. ISPAI members are keen ensure that the "right thing" is done in a considered and appropriate response.

However, there is disagreement among experts about the true nature and scale of the problem[1], the effectiveness of the blocking technologies to kerb the activities of those that pose a danger to children and the cost-benefit economics. The last point being particularly relevant in the context of encouraging competition to expand broadband penetration and develop e-commerce services in the economy. Unfortunately, reasoned debate on CP blocking is often made complicated and issues confused by the emotional reactions that are evoked by child protection issues.

Although the concept of ISPs blocking illegal content appears simple, and few would object to its intention when restricted to CP, implementation is complicated by a considerable number of legislative, technical and resource implications. It is vital that any agreement between Government and ISPs in Ireland to introduce blocking of CP on the Internet should be based on a thorough examination of all the implications.

The ISPAI wishes to work with Government to determine a balance of legislative and self-regulatory measures to provide an agreed framework within which ISPs could implement blocking of access to known child pornography where technically feasible.

3.2 Development of blocking capability

This matter has now become topical due to two main developments:

[1] That is the risk to the general public, especially children, of unintentionally encountering CP while using the Internet. This initiative will not directly prevent clandestine distribution of CP by paedophiles.

1. An established Hotline network providing professionally verified intelligence on the locations harbouring known CP content which can be compiled into a reliable block-list (with national precedents led by the UK) and,

2. An acceptably targeted technology which can block CP content based on such a block-list.

With Hotlines having been in operation for nearly a decade and pooling of knowledge through the INHOPE[2], an expert capability and methodology exists to systematically compile a verified list of web-site locations where CP is hosted on the Internet. Until recently, no consistent and reliable way to then accurately block the identified CP sites existed.

Network operators have always had the ability to crudely disable access to sections of the Internet from any point within their network. Such wide-effect measures run contrary to the principles of operation of open communications services in free and democratic societies. They also expose ISPs to legal claims for damages from innocent sites affected[3] by any such action. For these reasons blocking has been shunned by ISPs.

Since 2004, technologies have been developed whereby ISPs[4] can, with reasonably confined targeting, block casual users from encountering illegal child pornography (CP) stored within specifically known web-sites. One such solution “Cleanfeed” was developed and introduced in the U.K. by the ISP unit within BT. It is based on a block-list compiled and distributed by the Internet Watch Foundation (IWF) - the U.K.’s INHOPE member Hotline.

In the U.K. government recognition has been given to the IWF as a foundation approved to receive and investigate reports of CP and compile the block-list. Home Office backing exists for its supply to and handling by ISPs for the purpose of blocking. Other ISPs in the U.K. have been encouraged to introduce similar blocking measures by the Home Office. Implementation of “Cleanfeed” relies on ISPs having compatible network equipment and topology and this is causing problems for a consistent U.K. national roll-out of CP blocking.

EU and other developed countries are examining similar initiatives. To date some ISPs in four other European countries (Norway, Denmark, Finland and Sweden) and some other jurisdictions (e.g. Canada, China) have introduced blocking under differing legal arrangements. These use a variety of blocking techniques and some do not have a high degree of target accuracy. Many ISPs can not implement “Cleanfeed” or similarly targeted technology at present. If forced by legislation to introduce blocking with short notice, these ISPs would have to resort to the cruder and more damaging techniques.

BT has offered to implement the same system at its Irish subsidiary, in the context of an appropriate government agreed framework for operation, and has asked the Department of Justice to consider this. Vodafone has announced its desire to implement blocking on its European networks using the IWF supplied list. Both are members of the ISPAI.

When examined, the seemingly clear-cut and worthy ideal of blocking child pornography has many far-reaching implications. These are particularly relevant if blocking CP was used as a precedent to justify calls for curtailment of public access to other forms of information that various groups may consider socially undesirable. The implications impinge on fundamental democratic and constitutional principles, and entail legislative, competitive, resource availability, technical and public expectation issues that must be addressed to support any national decisions to implement CP blocking.

[2] INHOPE the international network of Internet Hotlines which facilitates rapid exchange and action on verified reports of CP content hosted or distributed on the Internet.

[3] Previously available techniques generally result in wide “collateral damage”, that is many innocent web-sites and services, sharing the same domain or IP address but unconnected with the target illegal content, are also rendered inaccessible.

[4] Typically consumer-oriented ISPs having appropriate equipment and network topology

The ISPAI believes that:

- In principle, blocking of illegal child pornography content is a worthy objective.
- Blocking of illegal content (including child pornography) to be imposed on public Internet communications services at the ISP level should be defined within legislation, have adequate governance and be subject to public accountability.

In this paper, the ISPAI presents the issues that have been identified by members that must be resolved with government to allow blocking technologies to be safely implemented by its members in Ireland.

3.2.1 Internet service for which blocking is proposed

There are many different services provided over the physical computer network that is the Internet. For example: e-mail, world-wide-web, chat, news-groups and peer-to-peer file sharing, to name the most common. Child pornography (CP) can be distributed or facilitated using any of these.

It is important to understand that the technologies described are aimed at blocking casual access to CP on the World-Wide-Web **only**.

This is because for the other services, no reliable technical system has been developed that does not impose unacceptable degradation of network throughput or generate wide collateral damage.

Because CP is illegal in most countries, the purveyors of this content tend to move it frequently from one site to another. This reduces the effectiveness of end-user computer filtering applications that rely on static filtering criteria. In the specific case of CP, the use of blocking technologies that rely on a dynamic list of identified URLs may be an effective supplement to existing filtering technologies.

The aim of blocking would be to reduce somewhat the possibility of users accidentally discovering illegal content on web-sites as they “surf the web”. While this could potentially impede slightly the criminal providers of CP, the primary objective is to protect our customers, especially children, from exposure to imagery of the sexual abuse of children.

3.2.2 Blocking not required for Ireland and many other jurisdictions

It must be emphasised that blocking is not required to deal with illegal content that might be hosted in Ireland, as the Hotline and ISPAI members act very swiftly to remove such material as soon as we are given knowledge of its existence. ISPAI members actively cooperate with An Garda Síochána when presented with a valid warrant to gather evidence to support investigations that may lead to the apprehension of those responsible for placing illegal content on our facilities.

The same system applies to child pornography found to be hosted in other jurisdictions which (like Ireland) are part of the INHOPE Hotline Network. The result of the existing INHOPE system is that illegal content is rapidly removed from the Internet by the jurisdiction in which it is located. The more jurisdictions that cooperate, the fewer havens there will be for criminals and paedophiles to host their illegal material.

Consideration of blocking is therefore only required to deal with content hosted in jurisdictions who, through inaction when notified, act as havens for illicit material which can then be accessed (usually inadvertently) by people world-wide using the Internet.

The ISPAI believes that Hotlines and ISPs, reacting rapidly in combination with law enforcement action, have proven to be very effective in reducing the hosting of child pornography on the Internet; as shown by statistics from INHOPE member countries5.

ISPAI would welcome diplomatic initiatives from the Irish Government and EU member states to encourage further countries to join INHOPE and adopt this approach and so disrupt criminals and paedophiles from utilising the Internet for the distribution of child pornography.

3.2.3 Outline of blocking implementation and scope

To understand the implications and issues described in the following sections, it is necessary to have an overview level understanding of the operation of the Internet's IP addressing and domain name systems. This overview is provided in Appendix 1.

Research is being conducted in many organisations on new technologies that may provide automated means of recognising illegal content and then filtering it out. At present these are all too unreliable to be considered for implementation by ISPs. However, many filtering packages are available for end-users to install on their computers. ISPAI members have actively encouraged such end-user filtering.

Current technologies that can be used by ISPs rely on block-lists or allow-lists which are manually compiled and can then be applied within the ISP infrastructure to selectively block the web access it provides to its customers.

There are different techniques utilising a block-list that can be implemented by ISPs to achieve blocking. These are:

- IP address blocking
- DNS blocking
- Targeted hybrid blocking (e.g. BT Cleanfeed[6])

Each yields differing results in terms of effectiveness, ease of circumvention and collateral damage. Appendix 2 outlines these techniques and their affect.

The block-list itself is also manually compiled and consists of specific web-site addresses (URLs) identified by Hotline Content Analysts as containing child pornography (CP) and not being taken down within a reasonable time. This information is then supplied to a compiling authority. In some jurisdictions the compiling authority and Hotline are the one body. Due to the nature and sensitivity of the block-list there are many issues around its security, distribution and handling by both the compiling authority and ISPs. Appendix 3 provides more detailed information on list related issues.

In general, blocking can prevent the casual Internet user from accidentally encountering the block-listed sites when "surfing the Web", using search engines or when such material is linked from another source. For example, if the user clicks a link to a block-listed site presented in a spam e-mail or on a search engine results listing, the browser invoked will fail to retrieve and display the data.

Targeted blocking technology only works against world-wide-web sites and generally cannot be scaled across larger networks. Typically it can only be implemented by certain ISPs, generally those with smaller networks and an end-user focus. Mobile operators offering i-Mode as well as standard GPRS (WAP) access have particular difficulties to implement consistent blocking between the two services and would have to develop additional list

[5] IWF figures for illegal content reported to their Hotline and traced to the UK had dropped from 18% in 1997 to just 0.2% in 2005. www.hotline.ie has never had a report where illegal content was traced to a host in Ireland.

[6] ISPAI does not wish to promote any particular proprietary blocking system but due to the media exposure received by BT Cleanfeed it is necessary to indicate which class of blocking it represents.

translation systems. These favour “allow-list” systems which provide a “walled garden” Internet service.

3.3 Issues raised in considering ISP blocking

While the objective of the current proposal is the blocking of CP content, the technology can be applied to the blocking of any illegal content. The same technology could be misused to suppress access to any content by those with power over the system. Therefore the controls, checks and balances are vital to public confidence of any limited blocking system.

3.3.1 Questions of overall democratic and constitutional principles

The Constitution of the Republic of Ireland and the Treaties of the European Union, provide its citizens with certain rights of freedom, privacy, access to ideas and freedom of speech compatible with the principles of a liberal democracy. The Internet is rapidly becoming the primary source of information and preferred method of its distribution. The implementation of the technological capability to achieve blocking of identified Internet sources is therefore of immense gravity to fundamental democratic principles.

While the objective of ISP implemented blocking is raised specifically in the context of ISPs dealing with CP content (to which few would object), the technology introduces the capability to apply “hidden” censorship of citizens’ ability to access any chosen information from the Internet. Its consideration therefore sets important legal precedents.

While supporting the principle of ISP implemented blocking for the purposes of preventing or restricting access to child pornography via the Internet, ISPAI seeks clarification from Government of the legal basis on which such blocking would be carried out.

Internet blocking technology will prevent all persons within the State (under normal Internet usage conditions) from having access to information that resides at URLs which have been placed on a block-list. This block-list would be distributed nationally to be implemented by all ISPs in the State. No matter how worthy their intentions, those assigned to maintaining the block-list (effectively censors) are responsible for deciding what URLs are placed on it. This is a centrally imposed censorship function. The ISPAI does not consider this a function appropriate to commercial organisations.

ISPAI therefore believes that the Government must consider a structure where the powers of censorship (i.e. authorisation of and responsibility for the blocking list) are vested in a State authority. This body must be accountable to the Oireachtas and have an appeals process to ensure public confidence that centrally imposed restrictions on the Internet are not being misused and are applied in accordance with constitutional principles.

It must be emphasised that the intentions of child welfare pressure groups and those ISPs who are seeking to implement Internet blocking, are strictly to combat the dissemination of child pornography over the Internet. This is being done with the following objectives:

1. To reduce the chances that citizens, particularly children, encounter images that are actually illegal and that most find to be abhorrent.

2. In reducing ready access to known child pornography sites, to kerb its availability on the Internet; a factor which many commentators believe would assist in reducing demand.

3. By kerbing the market for child pornography on the Internet, to assist in reducing the amount of the physical and sexual abuse of children, no matter where they live which, by definition, must occur in order produce illegal images and video content that constitute child pornography.

The intention of ISPs is that the proposed blocking must be confined strictly to content that is illegal under the Child Trafficking and Pornography Act (1998 to 2005). ISPs are very concerned that when it is widely known that capability exists to block material, pressure groups from every quarter will try to bring pressure to bear on the industry to block content with which they disagree and believe to be illegal.[7] As commercial organisations, ISPs could be placed in an untenable position.

ISPAI therefore seeks the assurance of Government that it can support means, that are in line with the constitution and law, whereby the scope of blocking can be contained and strictly confined to content that is illegal under the Child Trafficking and Pornography Act (1998 to 2005).

3.3.2 Legal issues on the principles of blocking

Assuming in principle that blocking could be undertaken, the ISP industry believes that it must be protected in law from the consequences of carrying out blocking initiatives on behalf of the State. Those involved with the production and use of CP are treated as such outcasts of society, that even the suggestion that someone may be a paedophile, or in some way assists them, can destroy reputations and lives. Accordingly Directors and employees of ISPs and the Hotline need assurances on a number of issues if they are to be involved with measures dealing with CP.

The block-list requires considerable resources to compile. It is probable that the most pragmatic approach is to import an existing list from another jurisdiction. This may then be modified by the compiling authority prior to its implementation by ISPs.

ISPAI seeks the opinion of the Government's legal advisors on whether the importation, distribution and hosting, by ISPs, of address information pertaining to known illegal child pornography web sites, necessary to achieve their blocking, would come under the exception in Clause 6 (2) (b) of the Child Trafficking and Pornography Act (1998 to 2005).

The block-list once imported would have to be distributed to many ISPs operating in the State to achieve blocking. This is contrary to the principle of containment. Access will have to be given a number of employees in each ISP that receives the list to implement it on routers and URL checking/filtering computers. It is inevitable, that at some stage, paedophiles or criminal organisations would seek to position themselves or accomplices in such positions. While ISP management would take every effort to ensure security, legislation does not appear to provide protection to ISPs.

ISPAI seeks the opinion of the Government on the possibility of legal protection of the Directors and Management of ISPs and Hotline where a breach of security happens unless there is a case of intentional misconduct on their part.

A block-list imported from abroad may contain URLs that are not illegal under Irish law. The scenario exists therefore that ISPs could be found to be blocking material that should not be blocked and accusations made against the industry of acting improperly. It is not impossible to envisage sharp practice to exploit such vulnerability for financial gain through legal actions for damages due to loss of revenue.

[7] This may occur where content held in another jurisdiction is not actually illegal itself but legal entities claiming to be rights holders may claim its accessibility to Internet users in this country without appropriate royalties being paid is illegal distribution and so should be blocked. Another example are recent laws enacted in Italy and some States of the USA mandating blocking of web-based gambling sites. There is political pressure in various EU States, from campaigners on such diverse matters as abortion, animal-rights and extreme right-wing or left-wing policies, to block web-sites which contain references to items that are illegal in their country.

ISPA seeks the establishment of a mechanism whereby the imported list can be reviewed to ensure it does not contain URLs that are not illegal under Irish law and that the block-list is approved by a State authority prior to distribution for blocking implementation by ISPs.

Under the e-commerce act, 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.

It is very possible that through reports made to ISPs within the State, e.g. to the www.holtine.ie service, that ISPs would have knowledge of illegal URLs hosted outside the jurisdiction that do not appear on any imported block-list. At present, despite that knowledge there is no mechanism that ISPs can use to remove those sites from public access and no obligation exists in law to do so. Blocking based on an imported list would introduce a mechanism whereby effectively “removal from access” could be carried out. If the State relied solely on an imported list, the additional sites of which Irish ISPs have knowledge would not be blocked and it could be seen that the Irish ISPs were not meeting their obligation under the law.

Therefore, in the opinion of the ISPAI, there needs to be a State approved method, whereby URLs of which the Irish ISPs have knowledge may be added to the list and approved by the State authority before it is distributed to ISPs for implementation.

ISPAI therefore requests that the Government provide a legal mechanism to allow a facility which operates in a proactive manner on behalf of the ISPs (the most obvious being the current Hotline) to check the block-list and to include URLs of illegal content of which it has knowledge, but which do not appear on the imported list, prior to its approval by a State authority for distribution to ISPs for blocking implementation.

Due to the scale of hosting operations it is not economically viable for the hosting provider to monitor all customer websites to ensure compliance with acceptable usage policies. If the user is a commercial operation holding third party personal and financial details, it may often be illegal for the Hosting ISP to do so. This is recognised in “the mere conduit” clauses of the e-commerce act. The ISPAI is extremely concerned that any actions, whereby the industry acts positively to block known CP content, could be construed as precedent which erodes the legal protection provided to any Telecommunications and Internet Service Provider as a “mere conduit” under the e-commerce act (i.e. transposition of e-commerce directive).

ISPAI therefore requests that the Government provide a legal assurance that activities to achieve blocking of illegal child pornography, and refusal to act similarly for other alleged illegal content, will not affect the “mere conduit” status of Telecommunications and Internet Service Providers.

3.3.3 Public liability issues relating to blocking

If blocking is to be established in part under a self-regulatory regime, ISPs must have indemnity from legal challenge for carrying out this public service. This is required due to the possibility of legitimate sites being inadvertently blocked for several reasons including: clerical errors in the URLs listed; occasions where legitimate site domain names or IPs have been temporarily “hijacked” when a blocking decision was made; where technological routing errors arise; or, when the content in question is subsequently found by a court not to be illegal under Irish law.

In such circumstances an owner of an inadvertently blocked site may claim damages for defamation, due to the grave implications that they must have been involved in the distribution of child pornography and/or for the possible loss of revenue during the time the site was blocked. This loss could be attributed to degradation in product or brand awareness and, if it is a transactional site, direct loss of potential earnings from the Irish market.

ISPAI believes for ISPs to be able to perform public blocking services there must be legal assurances that ISPs and the Hotline will have exemption from possible legal action for inadvertently blocking of legitimate sites, provided this has not occurred because of intentional misconduct on the part of the ISPs or Hotline.

If a blocking initiative is implemented, then there will be a public expectation that illegal child pornography URLs are being blocked by ISPs. There is a high probability (almost a certainty) that each month a majority of URLs containing illegal child pornography that exist on the Web will not be blocked. This is simply because they remain unknown due to CP distribution being a clandestine activity. Even the most restrictive filtering software (designed to identify legal pornography sites for child protection) blocks about 94 percent of sexually explicit search results, but also blocks about 13 percent of the clean results. (Stark).[8] A small number may also be unknown because they are newly re-established after being removed from a list or they were unintentionally not blocked (due to technical difficulties or clerical errors). It is impossible to ensure that 100% (or even a significant percentage) of CP URLs will be successfully blocked (and CP on all other non-HTTP services are not blocked by the current technology).

ISPAI believes for ISPs to be able to perform public blocking services there must be legal assurances that ISPs will have exemption from legal action taken by members of the public (or on behalf of minors) for exposure to illegal child pornography which they believe should have been blocked under the proposed public blocking service.

3.4 Resource and market issues

Given the variety of business models and technical infrastructures deployed by the ISPAI's members, it may not be possible, either technically or financially, for all ISPs to implement any blocking initiatives quickly or at all, especially on current equipment.

No uniform or standardised approach to implementation can be assumed for at least the next five years. Therefore flexibility is required until such time as the technical and network topology mechanisms to facilitate such blocking become industry standard.

ISPAI believes that a flexible framework would have to be developed that would allow for staged implementation by ISPs and that the full protection of the e-commerce directive will apply. It is important that ISPs (whether ISPAI members or not) should be free to decide whether to implement filtering or not, based on technical and commercial considerations.

If the ISPAI www.hotline.ie service is selected as the appropriate organisation to assemble URLs for the Irish block-list, prior to it being sent to the State authorising body, additional resources to maintain this function and indemnity would be required by the Hotline. These have already been outlined in a separate document provided to the IAB.

If the government decides that it should follow some countries and introduce mandatory blocking by ISPs, it must be cognisant that the cost of implementation could be prohibitive for some ISP to remain in business. The ISPAI believes that in the interests of the roll-out of broadband and stimulation of competition, financial support and tax allowances should be made available to ISPs for the initial implementation of blocking in such circumstances.

[8] Expert Report of Philip B. Stark, Ph.D., Professor of Statistics at the University of California, Berkeley, 8 May 2006, ACLU v. Gonzales (Civ. Action NO. 98-5591 (E.D. Pa.) An analysis of effectiveness of Internet content filtering prepared on behalf of the U.S. Fedederal Government's effort to sustain the Child Online Protection Act (COPA).

In the interests of competition and avoidance of market distortion, any legislation or statutory instrument that would mandate CP blocking must be issued to all ISPs offering retail provision of IP connections. (That is the customer is not themselves reselling, whether or not for reward, IP connectivity outside of their home or organisation. If they are reselling, they constitute an ISP and must be subject to the same legislation or statutory instrument to provide blocking.)

Legislators must be cognisant that any form of blocking order that applies only to selected ISPs could result in distortion of the market for ISP services. It could also result in loopholes that could be specifically exploited by criminals or paedophile rings.

Inward business investment of Internet and e-commerce services must be sustained to support the Irish economy. If legislation requiring blocking of CP were to be enacted without appropriate technical exceptions, efficiency of international data transit through Ireland and other international Internet based services could be severely affected, possibly to a level where such carriers or providers would be forced to relocate. It should only apply to delivery of retail customer connections.

To protect Ireland as a centre for Internet and e-commerce services, legislation or statutory instruments requiring blocking should only refer to the retail supply of Internet access services. That is, where the intention is the supply of Internet connection to an end-user customer.

3.5 Conclusion

This information paper has sought to highlight the serious technological, financial and legal issues presented by any potential content blocking scheme. The ISPAI is concerned that the repugnant nature of CP could overshadow reasoned debate to evaluate these issues and develop proportionate CP blocking measures. However, it is paramount that prior to the introduction of any private sector initiated content blocking or any government mandated content blocking, that all of the issues discussed in this paper be resolved to the satisfaction of all interested parties.

The implementation of URL blocking is feasible, however, no system is perfect and effectiveness can never be seen to be static. An “arms race” grows up between measures to block and means to bypass which evolve over time. Nevertheless, ISPAI believes that within the right legal framework it is appropriate that ISPs support governments to proactively disrupt the perpetrators of CP on the Internet.

It must be realised that ISP initiatives, if operated in isolation, can never provide a solution to the distribution of CP over the Internet. These can only be effective as part of wider action that must involve payments organisations and international law enforcement cooperation. While clandestine activities of paedophile rings may be little affected, if organised criminal involvement can be disrupted out of profitability the incidence of CP being encountered by innocent Internet users would be greatly reduced.

The issues of indemnity for ISPs (by way of legal exemption) and the wider issue of the risks for private companies undertaking a role of implementing public policy, in this case the worthy one of preventing the dissemination of CP, need to be carefully considered at Government level.

ISPAI has therefore suggested a framework of legislative and self-regulatory measures which can work together to extend protection of the general public from encountering CP when using the Internet.

ISPAI believes legislation could make clear all of the uncertainties identified, e.g.

- Body or Authority empowered to maintain a block-list and oversee its use
- Legal basis for operating URL blocking
- Protections to be afforded to parties involved in operating URL blocking

The ISPAI believes it is only with the support of the Central Government, particularly with regard to resourcing and appropriate legal protection as outlined throughout the document that the prevention of inadvertent exposure to CP content in Ireland can be meaningfully addressed. If Government support for the proposed model is forthcoming, ISPAI members will act to protect the wider public good and will assist to the fullest degree possible within the legislative framework which it believes should be put in place.

Appendix - 1 Overview of IP addressing and domain naming

The Internet links computers together in a mesh with multiple connections to other computers. Each computer is assigned a unique number called its IP address. This is of the form 194.125.139.132. When a user connects to the Internet through their ISP, their computer is assigned an IP address and becomes part of the Internet and so is capable of sending and receiving data to communicate over it. Similarly a web-server located anywhere in the world is just another computer on the Internet and must be allocated an IP address by the ISP through which it is connected. Requests and responses for data on the Internet are simply routed by the ISP networks from one IP address to another. The ISPs maintain routing tables which instructs their equipment of how to reach all the active IP addresses on the Internet. It is possible to retrieve data over the web by using the IP address but it is not particularly user–friendly. As a user is routed to the Internet solely through their ISP, if it was necessary to block customers' access to certain IP addresses, the ISP could achieve this by removing the IP address from their routing tables.

The World-Wide-Web makes it very easy for users to retrieve information over the Internet from designated computers which are known as servers. They serve requests for pages of data compiled into web-sites. To make it easy to use the web-sites can have a recognisable name known as a domain name, such as “xyzcompany.com”. What is more one can retrieve a specific page of information from “xyzcompany.com” by describing the place within that web-site that the required information exists. This is of the form “xyzcompany/products/newwidget.htm”. This specific location is referred to as the Uniform Resource Locator (URL). The key to the Web is the Domain Name System that automatically translates the domain name to the IP address and allows a request to be made to the server at that IP address for the specific URL.

If a Domain Name has not been set up and registered it will not appear in the name server look-up tables. If a non-existent domain name is entered by the user, a “page not found” or 404 error will be returned. If an ISP was instructed to block a domain name a simplistic solution would be to remove this from their name servers so it appears as non-existent to their users.

Hosting companies have been established around the World that lease web-space on their servers. This allows companies, traders and individuals to have their own websites without having to invest in their own equipment. Such a Web hosting server has one IP address, but may contain many hundreds of unrelated web-sites. The owners of the web-sites are responsible for the content they put on their sites. Unfortunately, some people misuse these services by placing illegal child pornography on their web-sites.

Appendix - 2 Outline of blocking techniques and affect

There are a number of blocking techniques and variations on how these are implemented. They have differing results in terms of accuracy (i.e. targeting the identified illegal content), effectiveness of blocking and ease of circumvention. All are based on a manually developed block-list of URLs. These techniques are described in simplified form below.

Domain Name System (DNS) blocking

The URLs on the block-list are directly applied as a filter to the subscribing ISP's name-servers (the look-up table that equates names with real computer (IP) addresses). Effectively, the domain name (root of URL) is removed from the ISP's name-servers. If a user attempts to access content at that URL, an error message is received as if the URL did not exist (i.e. was never registered).

It is a partial blocking technique. It does not block access to the IP address on which the URL's content actually resides. Users who utilise the IP address directly or use another name-server, which can reside anywhere world-wide on the Internet, will bypass the blocking.

DNS blocking is broad in affect as all content on the domain will be blocked. This affects shared domain services (e.g. similar to geocities) where innocent owners' sites would also be blocked.

Summary: DNS blocking is a partial blocking technique, it is easily circumvented and can produce limited collateral damage particularly to public shared domain services.

IP Address Blocking

This requires the block-listed URLs to be translated to the IP addresses on which they reside by every ISP implementing blocking based on this list. The ISP must then use some technique to remove these IPs from the routing tables applied in all routers in their network. If a user attempts to access content at a URL that is on the block-list, the DNS system will recognise the URL as valid, as this is propagated internationally and is not being altered. The DNS will then return the IP address that corresponds to that valid URL. However when the request is serviced, the router will fail to find that IP address and therefore can not pass the data retrieval request to the destination host server containing the blocked content. An error message is received as if the IP address, that is the destination host, did not exist.

IP address blocking is very broad in affect as all domains hosted on the IP address will be blocked. This means many legitimate web-sites owned by innocent users that happen to be hosted at that IP address will be blocked. Hosting companies have been established around the World that lease web-space on their servers. This allows companies, traders and individuals to have their own websites without having to invest in their own equipment. Such a Web hosting server often has very large numbers of unrelated web-sites residing at one IP address.

While it is a complete blocking technique for access of the IP address from that ISP's network, it can be relatively easily circumvented by using proxy servers outside the jurisdiction that do not implement the blocking list. Prevention of that circumvention would entail also having to block all known proxy servers; this would involve blocking facilities that are themselves not illegal. IP address blocking will block all services at the IP address, not just the World-Wide-Web as the ISP effectively disabling part of the Internet infrastructure as viewed from that ISP's network.

Summary: IP address blocking is a full blocking technique. It is relatively easy for technically astute users to circumvent and can produce wide collateral damage particularly to shared IP web hosting services.

Targeted hybrid blocking

This type of blocking is a relatively new development and uses a hybrid of IP/URL approach and a two stage methodology. BT Cleanfeed is a targeted hybrid blocking system.

The advantage is that such blocking technologies are finely targeted and prevent access solely to the specific illegal content designated by the URL on the block-list. This can be as accurate as a single image or web-page.

As every web "get" request received by the ISP from all users has to be checked against the specific URL list, this places a very heavy additional load on the ISPs routing processes. If this was to be done at all input points users would notice considerable degradation in service. The system therefore uses a two-tier approach so only "suspect" requests are diverted to a special dedicated checking point.

The technology resolves the block-list URLs to their IP addresses and provides new routing for these IP addresses so that user requests are diverted to the dedicated checking point in the network. This first stage is automatically distributed to all user access routers on the network. This has no impact on performance. If a user request does not resolve to a "suspect" IP address it is routed uninhibited to the web-server and serviced as normal.

If the IP address of the requested URL is a block-listed URL (only a very small number of all requests), the request is routed to a central location where powerful computers can run the full URL check. If the URL is not a block-listed URL, the web-page request is serviced as normal via the dedicated checking location routers and the web-server responses are routed back to the user. If the URL is on the block-list, that is, it has been designated as confirmed child pornography, the request is not serviced and an error message is returned. In the case of BT Cleanfeed it was decided to provide a standard "404 Not Found" error. Alternative messages can be generated.

To avoid incorrect blocking errors, a hybrid blocking system should be fully automated. This largely depends on the equipment and resources available to the ISP. A given ISP implementation may require some elements to be manual and this introduces scope for unintentional but incorrect blocking. However, it must be remembered that no programming is perfect and even in a fully automated implementation there is always a possibility of an error occurring.

Summary: Targeted hybrid blocking is regarded as an accurate blocking technique. It is relatively easy for technically astute users to circumvent. It is unlikely to produce collateral damage especially where fully automated and allows access to legal information stored at the same IP and domain. It will prevent casual users from encountering illegal content designated in the block-list.

Allow-list ("white-list") option

Some providers offer an alternative solution to block-list based blocking. This entails providing a managed Internet connection as an optional retail service. This service restricts customer access to vetted and approved web-sites based which have been placed on an allow-list. By definition, everything else, including illegal content is effectively blocked. This service is currently offered by two mobile operators operating in Ireland (O2 and 3). It is also the method currently used by HeaNET in its managed service provided to Schools (but not Universities). It is only a retail solution and can not be applied at wholesale or transit ISP level. It can not be provided as an enforced solution on universal Internet services to the general public as it represents massively wide-spread censorship of content. It is only suitable as an opt-in service (which may be the default in certain circumstances, e.g. mobile service for young children) or where very restricted managed services are acceptable to the consumer and they knowing purchase this.

Allow-lists based systems, like any other, can not guarantee that illegal material could never be encountered. It is always possible for any website on the internet to be compromised and illegal material placed within it. The wider the circle of approved sites, especially if this includes blogs or other user-modifiable content, the greater is the possibility for compromise. The risk of such compromise has an extremely small probability of occurrence.

However, due to the sheer enormity and dynamic nature of the Internet and diversity of customer requirements, no allow-list can be effectively managed to include all legal material and exclude only illegal content. The solution is particularly restrictive and not suited to many business, research and home users. The benefit of the solution is it is possible to offer differing levels of allow-list which can associated with the user's logon so differing material can be offered to children of various age groups.

Allow-list based services by definition block everything except the specific URLs listed. Because these are legal sites and therefore their URLs can not be illegal, legal issues do not arise around the distribution of the list to implementing ISPs. By definition it represents massive censorship of possibly millions of legal web-sites, so can only be utilised in restrictive services to which the customer has agree.

Summary of blocking options

When considering a blocking technology, the cost of implementation must be considered relative to its effectiveness in having an impact and the probability of causing collateral damage. Many ISPs will have invested in developing a network topology and have equipment that is not readily suited to running a purchased targeted hybrid blocking system or could not sustain the cost of implementing a version that would work on their system could be prohibitive.

ISPs may not have the equipment or network topology that would allow the implementation of the targeted URL/IP blocking technology such as BT Cleanfeed or equivalent. Similarly it may not be possible or feasible to implement allow-list solutions. If the government requires blocking to be applied by ISPs, these ISPs would have to resort to an implementation of IP address blocking or DNS blocking. As these will cause collateral damage in many cases, legal exemption from action of affected parties would have to be provided.

Appendix - 3 Blocking list compilation and distribution

The block-list of CP sites used by ISP based blocking systems is derived from reports made by the public to Internet hotlines. These may be government approved civilian, government or law enforcement agency run services. The reports are of content that members of the public have encountered when using the Internet and which they suspect to be illegal. The Hotline professional content analysts will assess the content and decide whether these would be considered illegal under the law of their jurisdiction. If the URL does provide illegal CP the URL is recorded in a database and the source server is traced. Notice is sent to the jurisdiction in which it is apparently hosted.

The URL is also sent to the block-list compiling authority. The compiling authority checks whether the CP has been removed within a reasonable period. If it has not been removed, the URL is placed on the block-list. The compiling authority also regularly checks those already on the block-list to establish if the illegal content has been removed or the URL deleted. If the CP is not present for a set period, the URL is removed from the block-list.

The compiling authority is the body that has been given government approval to act on its behalf to decide what content should be blocked. In some jurisdictions the compiling authority is the civilian hotline (e.g. UK) in others it is the police (Norway and Denmark). It is conceivable that other public authorities such as a censorship board or regulator's office could be a compiling authority. Irrespective of which model is used, some form of legal protection must exist to cover both their work and the fact that they distribute the block-list to ISPs.

Allow lists do not contain references to illegal content as do block lists. Distribution of allow-lists presents little or no legal risk. Nevertheless in obtaining and compiling allow-lists staff will be exposed to illegal content and they and the organisation must also have legal protection.

If allow-lists or block-list are imported for use within the jurisdiction, it is very important that the compiling authority in the Irish jurisdiction has oversight and accountability for what the foreign compiling organisation is providing. At present most allow lists services (and filtering products) are provided by private companies located outside the European Union. Some services even send every web request made by a user to checking servers located outside the EU and return whether the site should or should not be accessed by the filtering system.

Clearly information contained in block-lists is extremely valuable to paedophile rings and criminal elements. Maintenance of security at Hotline, compiling authority and ISPs is therefore imperative. Staff should be vetted and I.T. systems secured. It is also best practice that the specific persons in the ISP charged with management of blocking and the staff that receive the block-list and actually implement the blocking service should also be vetted. (This is for protection of the ISPs and to save government embarrassment should a leak of the list occur). This is done in some of the jurisdictions currently practicing Internet blocking.

In preference, the system to distribute the list and implement it on the ISP infrastructure should be as automated as possible. The list should at least be encrypted and transmitted from compiling authority to ISP over a secure link. Current blocking systems use proprietary applications, the details of which are not made public for security reasons. Some claim that due to the specific equipment installed, the process of block-list receipt and application on their infrastructure is almost completely automated. In many cases it is not possible to apply the block-list to the ISPs routers and filter systems using a fully automated system and manual decryption of the list and programming of the URLs into routers and filter systems is required. Clearly the more manual intervention and the more people with access, the greater the risk of the contents of the block-list finding its way to criminals or paedophile rings. List source and management is a critical element of the blocking process.