Online Child Abuse Material

Effective Strategies to Tackle Online Child Abuse Material

September 2013

> *"A child abuse image is a crime scene, a digital record of some of the most monstrous crimes against children. This is about protecting real children from real abuse in the real world."*
>
> *Senator Jillian van Turnhout*

Acknowledgements

There are a number of people without whom this report might not have been written, and to whom I am greatly indebted. In particular, I would like to commend the steadfast work being done by individuals, NGOs and law enforcement agencies such as Pat McKenna, the Internet Watch Foundation, An Garda Síochána, Europol, and Interpol.

My sincere thanks to Adam Hurley and Amy McArdle for their assistance in writing this report.

I have made every effort to ensure that the information in this report was correct at the time of publishing. I have endeavoured to acknowledge sources for materials gathered during my research. If you believe I have made an omission or I have not correctly attributed a source please do not hesitate to contact me and I will work to rectify the information.

Published in Ireland.

www.jillianvanturnhout.ie
Email: jillianv.vanturnhout@oireachtas.ie
www.facebook.com/jillianvanturnhout
@JillianvT

Table of Contents

Foreword by Senator Jillian Van Turnhout

I firmly believe that the proliferation of child abuse material (CAM) on the internet is a stain on our moral conscience. This belief has motivated me to make tackling online CAM a priority in my work as an Independent Member of Seanad Éireann, where I have pursued the issue through a Seanad motion before the Minister for Justice and Equality, Alan Shatter TD, and adjournment debate with Minster of State for Disability, Older People, Equality & Mental Health, Kathleen Lynch TD. I have also written extensively on the issue in newspaper articles and blogs.

Concerned by the lack of progress on the issue, I commissioned the following report to outline the options available both to the State and Internet Service Providers (ISPs) to: tackle the proliferation of child abuse material on the internet; examine best practice and draw on the experiences of other jurisdictions; and expedite action to protect real children from real abuse in the real world.

In arriving at the overarching recommendation that the Government must introduce and support a filtering system against online CAM through legislation or statutory instrument, I am acutely aware that there is no panacea to either eradicate child abuse or its recording and redistribution as CAM.

However, I am confident that a statutory filtering system of CAM on standard webpages will have a significant impact by:

- Preventing the unfettered redistribution of CAM and thus protecting the abused children from repeated victimisation.
- Protecting the public from accidental access to online CAM.
- Preventing deliberate access to CAM via standard webpages.
- Creating barriers to CAM and thus deterring curious/simple viewers for progressing onto more serious levels of offending behaviour, such as trading.
- Sending out a clear and unequivocal message to victims, perpetrators and the public that CAM on the internet is not tolerated.

Senator Jillian van Turnhout
September 2013

Executive Summary

The following recommendations are drawn primarily from the findings of this report, and are informed by research, experience, and lessons learned in a number of other jurisdictions.

Recommendation 1: Government must introduce and support a filtering system against online child abuse material through legislation or statutory instrument, rather than using the threat of same as a means to coerce Internet Service Providers (ISPs) into self-regulation. Said legislation or statutory instrument must ensure that the filtering system complies with our international human rights obligations and should fully address any outstanding concerns around the filtering issue.

Recommendation 2: The cornerstone of any successful filtering system is public trust and therefore the system must be underpinned by transparency and accountability. It is crucial that the public is made aware of the system before it is implemented and is provided with an appropriate avenue for redress with respect to any grievances or complaints they may have over filtering decisions.

Recommendation 3: The objectives of the filtering system must be clear from the outset. It must be limited to what is practical and achievable; evidence based; and must address 'mission creep' concerns head on.

Recommendation 4: The system must include stop/warning pages. This serves a dual purpose. Firstly, it demonstrates a commitment to one of the core principals of the system, the prevention of unintended and unwanted access to offending material. Secondly, it ensures operational transparency insofar as when an individual arrives at a stop page, they know why they are being denied access and what can be done if they feel an error has been made.

Recommendation 5: The Government should work with large online search engines, such as Google, as well as the Internet Watch Foundation (IWF) to implement a filtering system with the most up-to-date technology. With recent developments in this area, and Dublin now regarded as the "internet capital of Europe", Ireland is in a unique position to adopt and develop the most innovative methods in filtering and put itself forward as a leader in this field.

Recommendation 6: The Department of Justice and Equality must transpose Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 combating the sexual abuse and exploitation of children and child pornography, and replacing Council Framework decision 2004/68/JHA as a matter of urgency.

Introduction

Child pornography is clearly defined under section 2 of the Child Trafficking and Pornography Act 1998. The definition encompasses any visual representation that shows a child engaged in, or being a witness to, explicit sexual activity and the depiction, for a sexual purpose, of the genital or anal region of a child. The image or depiction is a culmination of at least one, but more than likely a series, of the most serious criminal offences known to our statute books, crimes such as: rape; incest; assault; sadism; and bestiality.

While often referred to as child pornography, the author, mindful of the need to distinguish between the use of materials for sexual gratification and materials that record or depict the sexual abuse of a child, adopts the term "child abuse material". While a picture of semi-naked children playing on the beach may sexually stimulate an individual, it does not in of itself constitute child abuse material, which refers a visual record of abuse and degradation. Child abuse material is a digital record of a crime scene. Over time we have seen the nature of this material increase in extremity to a point where Interpol are now regularly finding images and videos of children so young the nub of their umbilical cords are still visible (Moran, 2011). Indeed, it is believed that abusers are purposely selecting children from this age group, as they are too young to articulate the abuses being perpetrated against them.

With acts such as these in mind, it is clear that the proliferation of online child abuse material must be tackled as definitively and proactively as possible. However, as countries around the world attempt to limit access to and the spread of child abuse material though online filtering, Ireland's approach to the issue has remained troublingly laissez faire.

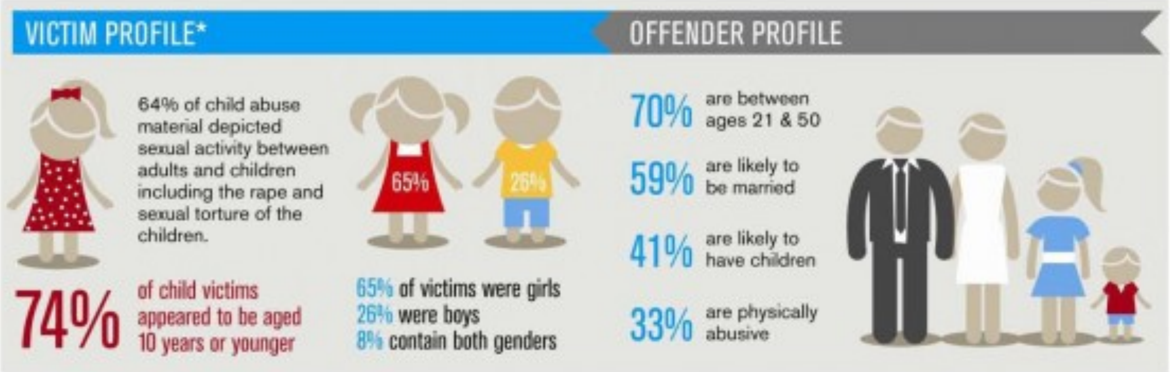
This Report aims to outline the options available both to the State and Internet Service Providers (ISPs) to: tackle the proliferation of child abuse material on the internet; examine best practice and draw on the experiences of other jurisdictions; and expedite action to protect real children from real abuse in the real world.

Background

Child abuse material has existed in one form or another since the advent of the camera in the late 1800s. However, due to a lack of child specific legislation following the decriminalisation of pornography production in Scandinavia, the 1970s saw a sizable peak in its commercial availability in Europe and the United States. The introduction of targeted legislation in Denmark and Sweden in 1980, and the Netherlands in 1986, effectively ended the commercial distribution of this material as the main means of supply, but it was quickly replaced by an increase in the non-commercial trading of images. The practice was significantly exacerbated by the phenomenal rise of the internet, which made access to images of child abuse far simpler and their availability more widespread. In 1995, Interpol was aware of 4,000 child abuse images in total. Recent data puts the number of known images at over 1,000,000. According to the National Centre for Missing and Exploited Children in the United States, the number of child abuse images on the internet increased by 1,500% between 1997 and 2003. It is now estimated that 750,000 people are using websites showing images of child sexual abuse at any one time (Maalla, 2009).

Victim and offender profiles

There is no atypical victim of child abuse hence there is no atypical victim of child abuse material. Children of all ages, ethnicities and genders are depicted and victim profiles vary dramatically between national organisations. For example, Canadian Customs found that 75% of the material they seized featured underage boys (Healy, 2008). While, in the UK, the Internet Watch Foundation (IWF) puts the figure of male victims at 10% (IWF, 2012). However, given its international component and sole focus the IWF gives to this issue, it is quite likely that their figures are more representative of online child abuse material as a whole and provides a stark insight into the nature of the material and its victims. In 2012, they estimated that 81% of victims were under the age of 10 years, a 6% increase on the previous year's figures. 10% of the material reported to them contained both genders, and in recent years up to 64% depicted sexual activity between adults and children including the rape and the sexual torture of children.



Identifying the consumers of child abuse material is a more complicated endeavour since, unlike the victims who are actively depicted, we cannot ascertain data from the image or material itself. Of those convicted of relevant offences, 70% are between the ages of 21 and 50. At 59%, the majority of viewers are married with 41% deemed likely to have children of their own. Of this group 33% are also suspected of being physically abusive towards their own children (McKenna, 2011).

Filtering

At its simplest, filtering child abuse material online works by comparing the requested destination of a user against a list of sites that are known to contain offending material and re-routing that request where necessary. While filtering does not remove the content at source or block all forms of digital distribution, this is not the aim of a filtering model. Rather, the aim is to protect the identity of victims and to create a preventative barrier to accessing the material, specifically to reduce the likelihood of a so-called 'simple viewer' progressing into traders and experts. As this is a preventive measure, we must be mindful that law enforcement agencies do not see filtering systems as a substitute of traditional policing methods such as 'investigations into and the removal of child abuse material hosted on the internet, undercover operations, arrests, searches, and so on' (Interpol). Instead they are widely viewed by law enforcement agencies, both at home and abroad, as being a vital component of a holistic approach to combating child sexual exploitation and abuse.

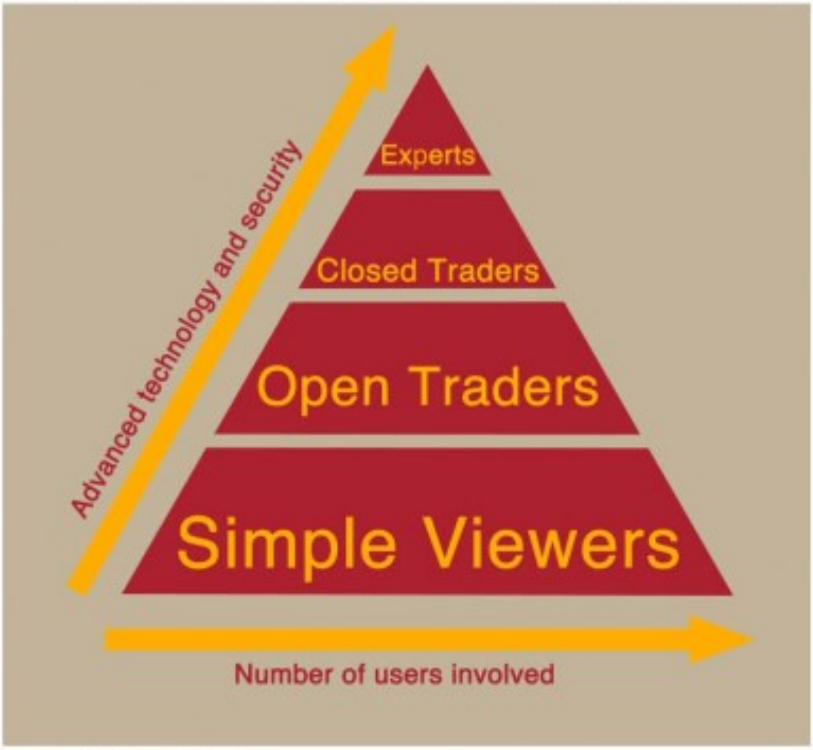


Figure 1: Moran (2011)

Technical Specifications

The filtering process relies on a manually compiled list of locations of child abuse material. In jurisdictions that implement blocking, there is some degree of variation around the information they choose to include. Differing methods of compiling lists include: full domain names; individual URL of sites found to contain child abuse material; and numeric IP addresses. While it is possible to install a filter at the national level, for example in China and Saudi Arabia, such a measure is usually adopted in order to filter wider content. Filtering systems that focus specifically on child abuse material tend to rely on the cooperation of the individual ISP to install the filter itself, thus affecting the customers of that individual ISP. After this process has been completed, when an individual attempts to access a site included on the black list of sites, their ISP diverts their request away from the offending content to either a standard "page unreachable" message, or a police "stop page" explaining why they are unable to access their requested site (Eneman, 2010). From a technical perspective, this is achieved one of three ways:

1. Packet Dropping

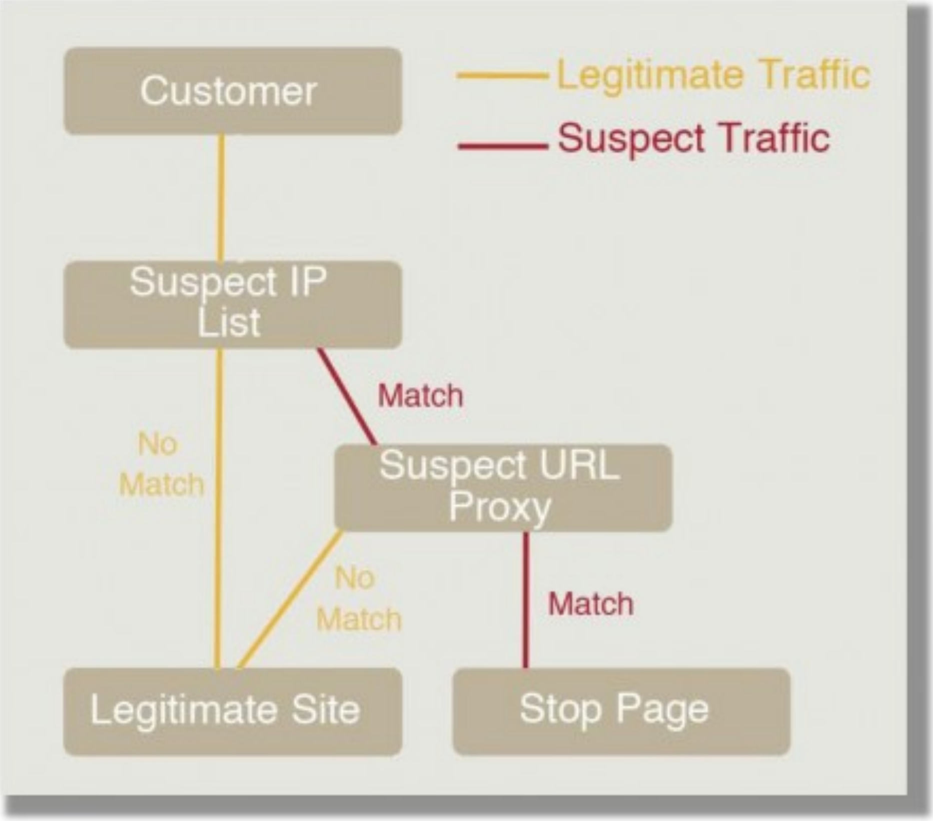
Packet dropping works from a list of IP addresses of websites that there is an intention to filter. Attempts to reach this IP address are discarded or dropped, thus preventing a connection to the server. However, the simplicity of this system also causes several difficulties. First and foremost is that all content at the targeted IP address will be filtered, rather than just the specific content. As Edelman (2003) notes, "87% of active domain names are found to share their IP addresses (i.e. their web servers) with one or more additional domains, and more than two third of active domain names share their addresses with fifty or more additional domains." Consequently packet-dropping systems run the significant risk of inadvertently "over blocking."

2. A DNS-filter/DNS Poisoning

The DNS (Domain Name System) is used by internet users to convert user-friendly domain names such as oireachtas.ie, into numerical IP addresses needed to locate the site online. In effect they are the phonebook of the internet. If a user attempts to access a blacklisted site using its domain name, the DNS filter will return a predetermined IP address, which does not correspond to the blacklisted site, thus redirecting its traffic (Zittrain and Edelman, 2003). This method suffers from a higher degree of over blocking as all the content on a particular domain is blocked. For example, if offending content was found on a hosting site such as the, now defunct, geocities.com, the blocking of this site would result in the blocking of millions of other innocent sites. While those who implement this system do take steps to address this issue, it remains an inherent issue, which should be noted. Furthermore, this method only affects the host name of the site. Consequently URLs containing the IP address would still be accessible.

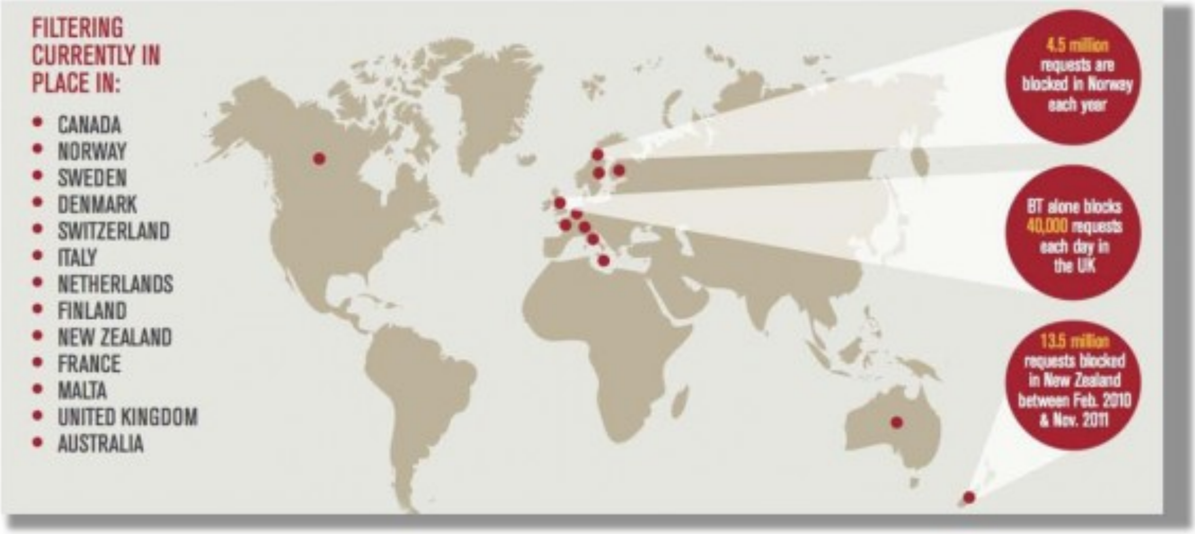
3. Proxy Filter

The proxy filter combines aspects of both the DNS filter and packet dropping methods and uses a two-stage filter system.



In the case of a proxy filter, all traffic undergoes assessment in a similar manner to a packet drop system. If there is no match, the traffic is directed on to its requested destination. However, if the requested destination is found to be included on the list of IP addresses suspected of hosting offending content, rather than simply denying the request as would be done in a packet drop system, the traffic is diverted to an additional proxy. This proxy then compares the requested URL to a pre-collated list of offending URLs. If the requested URL is not found on this list, traffic is allowed to pass on to its requested destination. However, if it is found to be on the list of URLs known to contain child abuse material, the traffic is redirected away to a predetermined location. This allows for the blocking of specific pages and file directories, rather than entire domains (Clayton 2006).

Current filtering systems


FILTERING CURRENTLY IN PLACE IN:
• CANADA
• NORWAY
• SWEDEN
• DENMARK
• SWITZERLAND
• ITALY
• NETHERLANDS
• FINLAND
• NEW ZEALAND
• FRANCE
• MALTA
• UNITED KINGDOM
• AUSTRALIA
4.5 million requests are blocked in Norway each year
BT alone blocks 40,000 requests each day in the UK
13.5 million requests blocked in New Zealand between Feb. 2010 & Nov. 2011

While regional differences exist in regard to which of the above methods are employed, for the most part child abuse material filtering systems can be divided into two distinct models: the Norwegian model and the British model. The former tends to operate as a voluntary public/private cooperation between the police and the ISPs to block domains, while the latter relies on self-regulation by ISPs supported by a national NGO to block URLs.

Only a small minority of these filtering systems operate with a statutory underpinning and consequently, in the relatively short time the systems have been operating, a certain lack of clarity has emerged regarding their legal status (Stol et al, 2009). For example, in 2004, the US District Court for Eastern Pennsylvania struck down a statute requiring the filtering of sites containing child abuse material. It found that it amounted to "prior restraint", which violated the First Amendment to the US Constitution (Center for Democracy and Technology, 2004). However, outside of the United States, models derived from the British and Norwegian models have proved to be more stable.

EU CIRCAMP

In Mainland Europe, the most common form of internet filtering is based on the European Commission funded CIRCAMP model, which introduces blocking at the ISP level based on a list of appropriate sites derived from Interpol's 'Worst of' list (McIntyre and Scott, 2010). Criteria for inclusion in this list is far more stringent than that of national lists due to the need to select benchmarks of illegality applicable to most, if not all countries. Thus, inclusion of material in the 'Worst of' list is predicated on the following:

• *The children are real. Sites containing only computer generated, morphed, drawn or pseudo* *images are not included.*

- *The ages of the children depicted in sexually exploitative situations are (or appear to be) younger than 13 years.*
- *The abuses are considered severe by depicting sexual contact or focus on the genital or anal region of the child.*
- *The domains have been online within the last three months.*
- *The domains have been reviewed and found to fulfil the above criteria by two independent countries/agencies or more.*

(INTERPOL)

The origins of the CIRCAMP model can be traced back to Norway where, in 2004, the decision was made to pilot a child abuse material filtering system using a list compiled by the Norwegian police's National Criminal Investigation Service, and based on DNS blocking (Deibert and Rohozinski, 2010). Due to its success, Norway became the primary driver of the European CIRCAMP project, which assists national police forces in adopting their own Child Sexual Abuse Anti-Distribution Filters (CSAADF) modelled on the original Norwegian system. At present, this is in place in nine countries; Australia, Denmark, Finland, Italy, Malta, Norway, Sweden, Switzerland and New Zealand. "This is generally done on a voluntary basis by ISPs, without any legislative underpinning" (McIntyre, 2012, p 8).

Despite criticism that blocking at the domain level imposes an unfair onus on the domain owner and administrator to oversee the content hosted on its domain and subdomains, the majority of CIRCAMP projects have followed the Norwegian structure and implemented a DNS blocking system. Proponents of the CIRCAMP model argue that the block will only remain until the content is removed, explaining that they believe "this will motivate content providers on the internet to actively make an effort to avoid files with child sexual abuse on their systems/services" (INTERPOL). In cases where blocking the entire domain would place and undue burden on legitimate users, for example free hosting companies where the service has been taking advantage of, CIRCAMP members will notify the administrator, which usually results in the speedy removal of the child abuse material.

The CIRCAMP model places an emphasis on the use of stop pages, which normally contain information about the type of content the user's browser attempted to access, links to national legislation, contact information to complain about the blocking, and to the police. The intention of these pages remains preventative in nature. CIRCAMP state;

> *"access blocking is purely preventive, no investigations against persons are initiated as a result of an Internet user being blocked and the "stop page" displayed. Internet users that are accessing, distributing, sharing, trading or possessing child abuse material will be dealt with using traditional police investigative methods outside of the*

preventive blocking." (Ibid)

However, in participating countries the ISPs grant police access to records of when the "stop page" is displayed, albeit with the IP address removed to ensure the anonymity of the user. The purpose of these logs is to provide police with information on new sites and how best to distribute resources.

UK Cleanfeed

The current UK filtering system has been in operation since June 2004 and was developed under the official name of the British Telecom (BT) Anti-Child-Abuse Initiative (Clayton, 2006). Since 1996, the Internet Watch Foundation (IWF), a nongovernmental organisation funded by UK ISPs and the EU, has operated a hotline for reporting suspected illegal material, including child abuse material. Where a complaint is found to be valid, it is reported to the police. While this is a highly successful method of addressing domestically hosted child abuse material, it was ineffective in addressing material hosted outside UK jurisdiction, which remained dependent on the local authorities of the host location taking it down. This prompted BT to develop a new form of internet filtering, dubbed Cleanfeed, in order to block access to such material hosted outside the UK (Walden, 2010).

Cleanfeed operates using the two-stage hybrid design of redirection and proxies described earlier and allowed BT to provide the technological framework necessary to institute filtering of the IWF's list of sites found to containing offending imagery. According to Clayton, "it is intended to be extremely precise in what it blocks, but at the same time to be low cost to build and operate" (Clayton, 2006, p.2). The success of its initial trial, coupled with political pressure from advocacy groups and the UK Home Office's threat to introduce legislation, compelled other UK ISPs to enter into a self-regulation model, which resulted in the vast majority of home connections in the UK being subject to the blocking system. When users attempt to access a black listed page, all UK ISPs, bar one, return a generic HTTP 404 'page not found' response rather than explaining why this page has been filtered. Furthermore, the Cleanfeed system is deliberately designed to discourage the collection of user data as its goal is solely the protection of its customers, rather than providing evidence to the police.

Notably, this system has developed without any legislative underpinning, leaving a private body to determine the potential illegality of an image. Consequently, there are limited procedural safeguards and no judicial oversight or review of decisions. This lack of transparency became highly evident when the IWF added a Wikipedia article that contained a 1976 album cover depicting a nude prepubescent girl, only to rescind its inclusion five days later following media criticism.

Incidents of false inclusion are quite rare and where they do occur, it is often only for a short period since the IWF's blocking list updates twice daily. At any one time, the list contains between 500 and 1,200 URLs, with an average of 59 new webpages addeddaily. In 2010, the IWF Annual Report found the list contained 14,602 individual webpages over the course of the year.

Ireland

In Ireland, the Child Trafficking and Pornography Act 1998, as amended by the Criminal Law (Sexual Offences) (Amendment) Act 2007, and the Criminal Law (Human Trafficking) Act 2008, deal specifically with child pornography. However, neither piece of legislation addresses how to deal with child abuse material hosted overseas, where removal proves difficult or takes an unreasonable length of time through conventional law enforcement channels. For example, material that cannot be addressed through the INHOPE network, of which Ireland is a member. INHOPE is the international organisation of Internet Hotlines which allows internet users to report suspect content in the same vein as to the IWF in the UK. In Ireland, this is done through Hotline.ie. The website is funded and run by the Internet Service Providers Association of Ireland (ISPAI). Hotline.ie was established in 1999 on foot of recommendations by the Irish Government's Working Group on the Illegal and Harmful Use of the Internet (Hotline.ie). When content is reported to Hotline.ie, it is first assessed by in-house staff. If the material is deemed 'probably illegal' and is hosted in Ireland it is forwarded to the Gardaí and the ISP to ensure its removal. If the content is hosted in a foreign jurisdiction, which also subscribes to the INHOPE network, then the report will be passed on to equivalent hotline there. However, if the content is hosted in a jurisdiction without an INHOPE member, it is sent to the Gardaí, who then attempt to address the content through international law enforcement channels, thus leaving the content available in Ireland and dependent on the speed and quality of the law enforcement response in the country in question.

Consequently, there has been growing focus around this issue with both civil society groups and the Gardaí calling for the expansion of our current system to include a filtering system. These calls have been echoed in the political sphere, particularly within Seanad Éireann, where Senator Jillian van Turnhout has led the issue though an adjournment debate and motion tabled by the Independent Group of Taoiseach's nominees in February 2012. The motion sought the House's recognition of the seriousness of child abuse material and the commitment of Government to address this issue in line with our international commitments. Specifically, the EU Directive on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, which requires all EU Member States to take the necessary measures to ensure the prompt removal of any webpages containing or disseminating child abuse material hosted on servers within their jurisdiction and, once appropriate safeguards are in place, permits Member States to take measures to block access to internet users within their territory of webpages containing or disseminating child abuse material hosted on servers outside their jurisdiction. In response to the motion, the Minister for Justice and Equality, Alan Shatter TD, committing to fully consider blocking in the context of the, as yet unpublished, Sexual Offences Bill. To date, however, neither the Sexual Offences Bill, nor legislation in line with the EU Directive have been brought before the Oireachtas.

This is not to say that filtering does not take place in Ireland. At present, Irish mobile operators subscribe to the Mobile Alliance Against Child Sexual Abuse Content and already prevent their users from accessing child abuse material. While the name "Cleanfeed" has become synonymous with the British filtering systems, the list built by the IWF is the basis of the system used by Irish mobile operators, as well as search engines such as Google and Bing. It is a testament to the how little such systems impact the day-to-day experiences of internet users that most are unaware of these filters existence.

Recommendations

Recommendation 1: Government must introduce and support a filtering system against online child abuse material through legislation or statutory instrument, rather than using the threat of same as a means to coerce Internet Service Providers (ISPs) into self-regulation. Said legislation or statutory instrument must ensure that the filtering system complies with our international human rights obligations and should fully address any outstanding concerns around the filtering issue.

It is the author's conclusion that the most effective strategy to tackle online child abuse material is through the introduction of a filtering system with a statutory underpinning. The legislation or statutory instrument must clearly stipulate: the nature of the material that will be filtered; how the filtering process will work; and the complaints/redress mechanism. Without such measures, the long-term viability of filtering is somewhat precarious. For example, the Dutch government introduced voluntary DNS blocking in 2007. However, a governmental study conducted by Stol *et al* (2009) later suggested that this system and by extension the majority of European filtering systems, was operating contrary to the provisions of the European Convention on Human Rights as it lacked a specific legal basis. Indeed, the 2011 OECD Report *Freedom of Expression on the Internet* went further noting, "In the absence of a legal basis for blocking access to websites, platforms, and internet content, the compatibility of such agreements and systems with OSCE commitments, Article 19 of the Universal Declaration [of Human Rights], Article 19 of the International Covenant on Civil and Political Rights and Article 10 of the European Convention on Human Rights is arguably problematic" (Mijatović, 2011, p.25). The report went on to state that voluntary self-regulation without government oversight may be "contradictory to the conclusions of the Final Document of the Moscow Meeting of the Conference on the Human Dimension of the CSCE, in breach of Article 19 of the International Covenant on Civil and Political Rights and Article 10 of the European Convention on Human Rights unless the necessity for interference is convincingly established" (Mijatović, 2011, p.182).

Recommendation 2: The cornerstone of any successful filtering system is public trust and therefore the system must be underpinned by transparency and accountability. It is crucial that the public is made aware of the system before it is implemented and is provided with an appropriate avenue for redress with respect to any grievances or complaints they may have over filtering decisions.

The central aim of the filtering system must be to limit the impact on the day-to-day operations of the average user as possible. It is important that users remain comfortable with the presence of the filter. As it would be counter-productive to disclose the content of the blocking list, the nature of this system requires a great deal of public trust The best way to maintain and cultivate this trust is with a filtering system underpinned by transparency and accountability.

Recommendation 3: The objectives of the filtering system must be clear from the outset. It must be limited to what is practical and achievable; evidence based; and must address 'mission creep' concerns head on.

And

Recommendation 4: The system must include stop/warning pages. This serves a dual purpose. Firstly, it demonstrates a commitment to one of the core principals of the system, the prevention of unintended and unwanted access to offending material. Secondly, it ensures operational transparency insofar as when an individual arrives at a stop page, they know why they are being denied access and what can be done if they feel an error has been made.

Without a codified mission statement grounded by legislation or statutory instrument, there is a significant risk of "mission creep" and privacy issues becoming a matter of public concern, especially in light of recent revelations regarding the monitoring of individuals online activities in other jurisdictions. While certain filtering systems state their goal as the prevention of child sexual exploitation, assessing how well a system achieves such a nebulous goal is next to impossible (Stol et al, 2009). What can be claimed with some certainty is that filtering systems act as a deterrent to curious/simple viewers and those with a burgeoning interest in child sexual abuse material who are not privy to the organized networks of file sharers, traders and producers. By denying initial or early exposure, it may be possible to curtail access to the clandestine trading networks.

Thus, there must be no doubt that the purpose of filtering is a preventive measure only, insofar as there is no presumption of guilt on the part of those who arrive at the stop page.

However, within an Irish context, there has already been some controversy in this regard, as in a letter to the Irish Internet Providers supporting the introduction of a CSAADF system, the Garda Síochána acknowledged that users may have accessed a blocked site inadvertently, but requested that when such a situation arises the ISP would provide "details of other websites visited by the user" (McIntyre, 2013, p 286). While this is in line with the behaviour of other CSAADF systems and there was no intention of seeking identification details from the ISPs, it raises obvious privacy concerns regarding the possibility of inadvertently identifying users based on their internet history. In other jurisdictions, strong opposition to such measures has arisen from the ISPs themselves, who stress that the stated goal of preventing exposure renders the presumption of intent moot. BT, for example, have purposely minimised the amount of user data they collect (*ibid*), in order to restrict the possibility of expanding the scope of the system beyond prevention.

Recommendation 5: The Government should work with large online search engines, such as Google, and the Internet Watch Foundation (IWF) to implement a filtering system with the most up-to-date technology. With recent developments in this area, and Dublin now regarded as the "internet capital of Europe", Ireland is in a unique position to adopt and develop the most innovative methods in filtering and put itself forward as a leader in this field.

In relation to the technological specifications of the system, it is the author's opinion that the DNS blocking used by CSAADF is not the ideal method for replication in Ireland as it has several notable weaknesses when compared the model operating in the UK. Firstly, DNS blocking can be more easily circumvented using the IP of the site. Secondly, the design of the DNS based system can lead to over blocking due to the targeting of entire domains. While similar charges of over blocking have also been levelled against the British two-proxy system, following incidents such as the blocking of Wikipedia pages, this was due to administrative error rather than a fundamental flaw in the system.

The author is not advocating for a wholesale replication of the British model, believing it to be unsuitable. Nor is the author purporting to criticise the IWF or those using a CSAADF system, as many of the issues described above are a product of their systems origins, which is to be expected when introducing an innovative new approach to any issue. However, as Ireland is in a position to select best practices from a range of jurisdictions, one would hope we might be able to avoid some of the pitfalls and teething problems experienced by other models.

Similarly, if this system is introduced, we must be mindful never to become complacent as this is an area that is still undergoing rapid development. For example, Google recently announced their intention to create a global database of child abuse material, which they will then share with their competitors, ISPs and law enforcement agencies, in order to facilitate the removal of offending material. Google has also committed itself to establishing an information exchange system with other online companies to ensure that this list is as up to date as possible. Furthermore, it is expected that when this new database becomes operational later this year, it will draw on information provided by the IWF to "hash" images, meaning they will not only flag the image at a specific location but also all duplicates of that specific image (Barrett, 2013).

Recommendation 6: The Department of Justice and Equality must transpose Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 combating the sexual abuse and exploitation of children and child pornography, and replacing Council Framework decision 2004/68/JHA as a matter of urgency.

Bibliography

Brown, Ian, ed. Research Handbook on Governance of the Internet. Edward Elgar Publishing, 2013.

Barrett, David. Google builds new system to eradicate child porn images from the web. The Telegraph 15 Jun 2013. Accessed 05/09/2013. Available online at: http://www.telegraph.co.uk/technology/google/10122452/Google-builds-new-system-to-eradicate-child-porn-images-from-the-web.html

Center For Democracy & Technology V. Pappert Case No. 03-5051 (E.D. Pa. Sept. 10 2004) https://www.cdt.org/speech/pennwebblock/20040915highlights.pdf

Clayton, Richard. "Failures in a hybrid content blocking system." In Privacy Enhancing Technologies, pp. 78-92. Springer Berlin Heidelberg, 2006.

Deibert, R. & Rohozinski, R., 2010. Beyond Denial: Introducing Next-Generation Information Access Controls. In R. Deibert et al., eds. Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace. Cambridge, MA: MIT Press.

Deibert, R.J., J.G. Palfrey, R. Rohozinski & J. Zittrain (2008) Access Denied; The Practice and Policy of Global Internet Filtering. Cambridge, Mass: The Mitt Press.

Edelman, Benjamin. "Web sites sharing IP addresses: Prevalence and significance." Berkman Center for Internet and Society, February 2003.

Eneman, Marie. Internet service provider (ISP) filtering of child-abusive material: A critical reflection of its effectiveness, Journal of Sexual Aggression. Volume 16, Issue 2, 2010

Healy, Margaret A. "Child pornography: An international perspective." In World Congress against Commercial Sexual Exploitation of Children. Stockholm, Sweden, pp. 27-31. 1996.
Internet Watch Foundation. Annual Report 2012

Kleinschmidt, Broder. "An International Comparison of ISP's Liabilities for Unlawful Third Party Content." International Journal of Law and Information Technology 18, no. 4 (2010): 332-355.

M'jid Maalla, Najat. Report of the Special Rapporteur on the sale of children, child prostitution and child pornography. A/HRC/12/23, 13 July 2009

McIntyre, TJ 'Child Abuse Images and Cleanfeeds: Assessing Internet Blocking Systems' In: Research Handbook on Governance of the Internet. Cheltenham: Edward Elgar. 2012

McIntyre, T. J. and Scott, Colin David, Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility. Regulating Technologies, Brownsword, R., Yeung, K, eds., Oxford, Hart Publishing, 2008.

Mijatović, Dunja. Freedom of Expression on the Internet: A study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States. Organization for Security and Co-operation in Europe. 2011.

Stol, W.Ph., H.W.K. Kaspersen, J. Kerstens, E.R. Leukfeldt en A.R. Lodder (2009) 'Governmental filtering of websites: the Dutch case'. Computer Law & Security Review 25 (3): 251 – 262.

Walden, I., 2010. Porn, Pipes and the State: Censoring Internet Content. The Barrister, (44), pp.16-17

Zittrain, Jonathan, and Benjamin Edelman. "Internet filtering in China. "Internet Computing, IEEE 7.2 (2003): 70-77.

Web resources

"Access Blocking." INTERPOL. No Date. http://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking

"INTERPOL Crimes Against Children Team on EU Directive", CIRCAMP, No Date. http://circamp.eu/

"About the Hotline". Hotline.ie. No Date. http://hotline.ie/

Appendix 1 – Seanad Éireann Motion, 29 February 2012

Private Members Motion
Independent Group
29 February 2012

"That Seanad Éireann:

- Notes the adoption by the European Parliament and the Council of the European Union, on 13 December 2011, of the Directive on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA. Among wide-ranging provisions in relation to criminal offences and sanctions in the area of sexual abuse and exploitation of children, the Directive requires all EU Member States to take the necessary measures to ensure the prompt removal of any webpages containing or disseminating child abuse material hosted on servers within their jurisdiction. The Directive also, with appropriate safeguards, permits Member States to take measures to block access to internet users within their territory of webpages containing or disseminating child abuse material hosted on servers outside their jurisdiction.

- Notes that while Ireland has arrangements in place to secure the removal of child abuse material on domestic servers, and reports material found outside the jurisdiction via the INHOPE network, Ireland has not sanctioned a system which would allow the same material hosted overseas to be blocked, where removal proves difficult or takes an unreasonable length of time.

- Recognises that "[C]hild abuse images are not just images. Despite the fact that most of them can be found in a "virtual world", one must never forget that behind every image, there is at least one child who has been sexually abused in real life. Child abuse images involve a series of crimes ranging from the solicitation, corruption or trafficking of children for sexual purposes and various forms of sexual abuse perpetrated on children, to the distribution, collection and consultation of images of the abuse committed." [Council of Europe Parliamentary Assembly, Report of the Social, Health and Family Affairs Committee, "Combating 'child abuse images' through committed, transversal and internationally co-ordinated action, Doc 12720, 19 September 2011]

- Recalls with approval Ireland's ratification of the United Nations Convention on the Rights of the Child on 28 September 1992 and welcomes that Ireland promotes and supports activities aimed at the removal of webpages containing or disseminating child abuse material in Ireland and shares this information with other EU countries through the INHOPE network and through cooperation with Europol and Interpol.

Calls on the Minister for Justice and Equality to:

1. Commit to bring forward a proposal to Government to ratify the United Nations Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography, signed by Ireland on 7 September 2000;

2. Commit to bring forward a proposal to Government to ratify the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, signed by Ireland on 25 October 2007;

3. Bring forward legislation, without delay, to implement the Directive on combating the sexual abuse and sexual exploitation of children and child pornography, which, legislation should:

    a) Underpin efforts to combat sexual abuse and the sexual exploitation of children and child abuse material in cyber space;

    b) Ensure a victim identification database and management system is in place which is directed at identifying child victims, prosecuting offenders and disrupting crime networks;

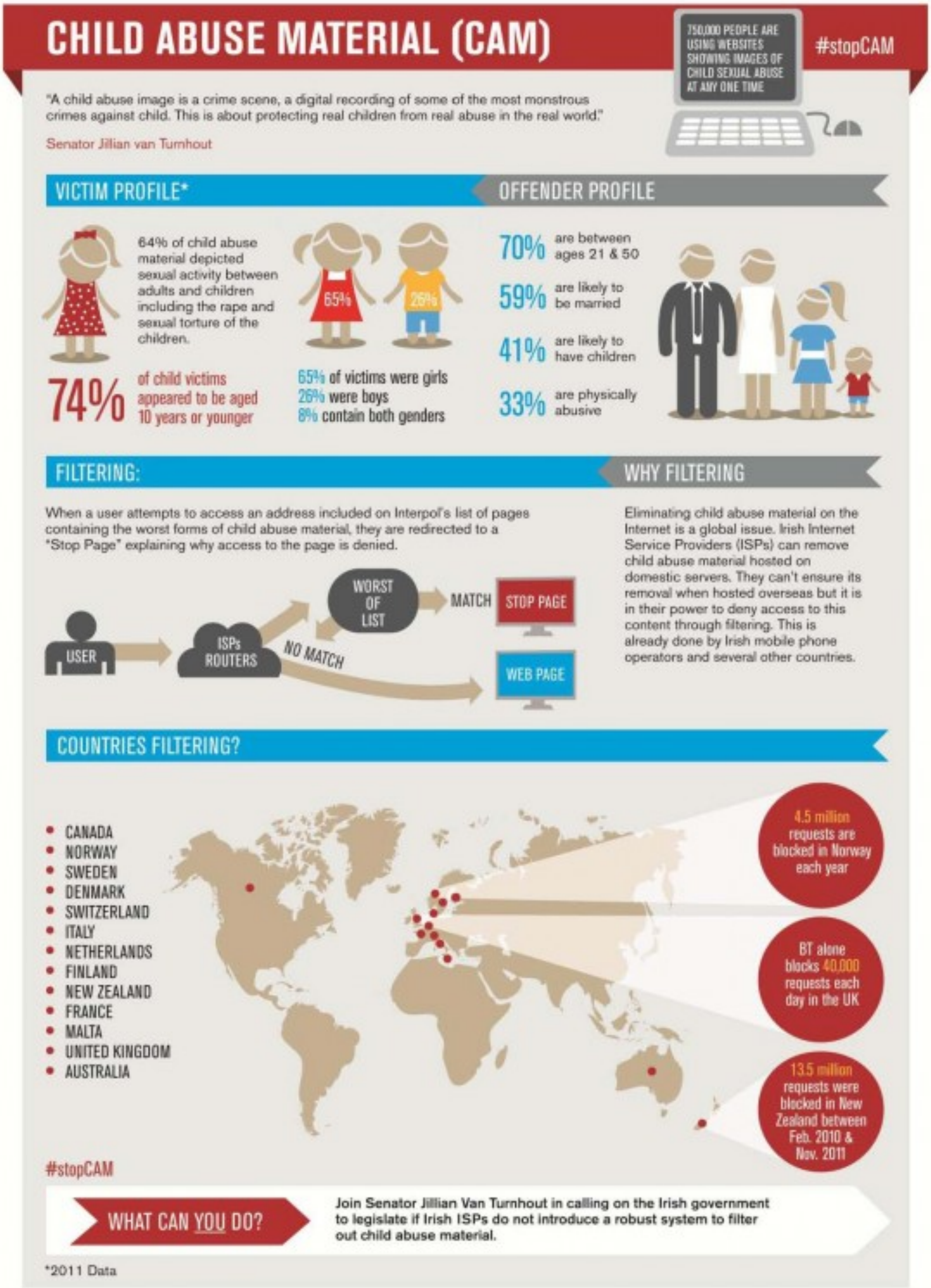
    c) Underpin measures already in place which seek to ensure the removal of webpages containing child abuse material hosted in Ireland;

    d) Direct that Irish internet service providers put in place a system whereby child abuse material, as defined by Section 2 (1) of the Child Trafficking and Pornography Act 1998, hosted overseas be blocked where removal proves difficult or is likely to take an unreasonable length of time; and

    e) Be guided by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction."

Senators Jillian van Turnhout, Martin McAleese, Fiach MacConghail, Mary Ann O'Brien, Marie Louise O'Donnell and Katherine Zappone

Appendix 2 – Infographic



CHILD ABUSE MATERIAL (CAM)

750,000 PEOPLE ARE USING WEBSITES SHOWING IMAGES OF CHILD SEXUAL ABUSE AT ANY ONE TIME

#stopCAM

"A child abuse image is a crime scene, a digital recording of some of the most monstrous crimes against child. This is about protecting real children from real abuse in the real world."

Senator Jillian van Turnhout

VICTIM PROFILE*

64% of child abuse material depicted sexual activity between adults and children including the rape and sexual torture of the children.

74% of child victims appeared to be aged 10 years or younger

65% 26%

65% of victims were girls
26% were boys
8% contain both genders

OFFENDER PROFILE

70% are between ages 21 & 50

59% are likely to be married

41% are likely to have children

33% are physically abusive

FILTERING:

When a user attempts to access an address included on Interpol's list of pages containing the worst forms of child abuse material, they are redirected to a "Stop Page" explaining why access to the page is denied.

WHY FILTERING

Eliminating child abuse material on the Internet is a global issue. Irish Internet Service Providers (ISPs) can remove child abuse material hosted on domestic servers. They can't ensure its removal when hosted overseas but it is in their power to deny access to this content through filtering. This is already done by Irish mobile phone operators and several other countries.

COUNTRIES FILTERING?

- CANADA
- NORWAY
- SWEDEN
- DENMARK
- SWITZERLAND
- ITALY
- NETHERLANDS
- FINLAND
- NEW ZEALAND
- FRANCE
- MALTA
- UNITED KINGDOM
- AUSTRALIA

4.5 million requests are blocked in Norway each year

BT alone blocks 40,000 requests each day in the UK

13.5 million requests were blocked in New Zealand between Feb. 2010 & Nov. 2011

#stopCAM

WHAT CAN YOU DO?

Join Senator Jillian Van Turnhout in calling on the Irish government to legislate if Irish ISPs do not introduce a robust system to filter out child abuse material.

*2011 Data