Combating online child sexual abuse content at national and international levels: IWF experience, tactical suggestions and wider considerations

1. Introduction

1.1. The UK Internet Watch Foundation (IWF) is often asked to contribute to national, European and international discussions and initiatives designed to improve responses to tackling child sexual abuse content on the internet. Wherever beneficial we share our model and expertise with organisations, companies, governments and agencies around the world to enable others to understand how the UK partnership approach and industry self-regulation is successful in the UK, as well as how the range of services we provide have helped to minimise online child sexual abuse content in the UK and beyond.

1.2. This paper sets out some of our views based on our experience of tackling the problem of online child sexual abuse content since 1996. It highlights issues that might assist policy makers particularly with regard to network level content blocking. It relies on our recent trends data to contextualise the problem and puts forward thoughts for effecting change in this area.

2. Background

2.1. The IWF was established in 1996 by the internet industry to be the UK internet Hotline for the public to report criminal online content within our remit in a secure, anonymous if desired, and confidential way. Our focus is to work in partnership with the wider online industry, law enforcement, government, and international partners to minimise the availability of specific criminal content in the UK but for the purpose of this document we concentrate solely on the primary element of our remit i.e. online child sexual abuse content hosted anywhere in the world.

2.2. In the UK it is a serious offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children. This includes downloading an indecent image to a computer screen. To the best of our knowledge downloading an indecent image of child to a computer screen wouldn't necessarily be an offence in many countries so whilst that situation prevails the demand for such content will thrive.

2.3. We are an independent self-regulatory body, funded by the EU and the wider online industry, including internet service providers, mobile operators and mobile manufacturers, content service providers, filtering companies, search providers, trade associations, and the financial sector. We work internationally with INHOPE Hotlines and other relevant organisations to encourage a global response to the problem and the wider adoption of good practices in combating child sexual abuse images on the internet.

2.4. Since 1996 we have managed almost 300,000 reports and have over 13 years' experience tracking and understanding the technologies, trends and movements behind the websites we deal with.

3. Content Trends

3.1. The nature, number, and profitability of child sexual abuse content on the internet are the subject of much speculation. In our opinion this content represents a relatively small proportion of total internet content and, although we believe the commercial distribution of such content is not increasing, it remains a very serious and persistent challenge.

3.2. This is an extremely fast-moving environment. Techniques used by criminals who sell, purchase, share or collect child sexual abuse images are sophisticated and are diversifying. Over half of the material we deal with is related to commercial payment mechanisms which we believe is indicative of an ongoing demand for images of children being sexually abused. Methods of operation appear ever more opportunistic. Distributers are increasingly exploiting apparently legitimate internet services to make the images available: from free or cheap hosting platforms and image sharing websites to social networking areas and hacked websites. We are aware of interrelated networks of child sexual abuse websites and their supporting payment and marketing platforms moving around the world and across hosting services regularly, frequently using automated or randomly generated systems to speed up and complicate hosting arrangements in an attempt to elude investigators. There is a persistent core of commercial 'brands' selling child sexual abuse images as well as technologically advanced and highly anonymised areas where images are shared and swapped on a non-commercial basis.

3.3. We suspect that the individual child sexual abuse web pages re-directing to an e-payment system which we take action against are providing a 'gateway' to many thousands of illegal images. This presents buyers with further opportunities to obtain content through ongoing membership and or to revisit and purchase more images.

3.4. As the distribution technologies and methods develop, tactics for combating them may become obsolete. Predicting the next distribution trend for the future is difficult. National police agencies have finite resources to carry out long-term investigations into large-scale global activities which span multiple jurisdictions, borders, and continents so it is essential that everyone who has a role in making the internet a safer place works together to tackle the problem.

4. 2009 figures

i. The IWF assessed 38,173 reports of alleged criminal online content.

ii. IWF took action on 8,844 occasions against web pages[1] containing child sexual abuse content, across 1,316 websites around the world.

iii. The majority of child sexual abuse content traced in 2009 was hosted in those areas with advanced, cheap and accessible internet infrastructures and services such as (North America, Europe and Russia).

iv. Less than 1% of child sexual abuse content known to the IWF has been hosted in the UK since 2003.

v. IWF issued 40 notices to companies to takedown child sexual abuse content in the UK and each notice was complied with within a day.

vi. 72% of the child victims in images dealt with by IWF appeared to be between 0 and 10 years old; 44% of images depicted the rape or sexual torture of a child.

vii. Over half the child sexual abuse content dealt with by the IWF was of a commercial nature.

viii. During the year, IWF identified at least 450 distinct criminal 'brands' selling images and videos of the sexual abuse of children, worldwide.

5. Dilemmas

5.1. There are a number of strategies and tactics which are making a difference in minimising the availability of child sexual abuse content and which, if adopted on a global scale could help ensure the international response to these crimes is more effective, faster and a better deterrent. Unfortunately, there is no international agreement on tactics so for example, some countries do not, to our knowledge, have an established system for the swift and effective removal of child sexual abuse content. Furthermore, debate continues in some countries

[1] This includes many individual child sexual abuse web pages re-directing to e-payment systems which provide a 'gateway' to many thousands of illegal images.

regarding what should be taken down, who has the right or authority to notify a company to remove it, and at what point in a potential investigation it should be removed.

5.2. In the UK, evidence of the content is captured and preserved for potential investigation following notification by the IWF and the content is swiftly taken down (usually within an hour of the hosting company receiving a notice). The IWF also provides a content removal alert service to its international members for non-UK hosted content and is considering other methods to speed up the removal of content hosted abroad. In the absence of consensus outside the UK we are prepared to work with foreign ISPs and hosting providers willing to join our organisation to help them rid their networks of such content. Any partnerships would be tailored to ensure they would not compromise any judicial or law enforcement arrangements in the jurisdiction where the content appears to be hosted.

5.3. One global law enforcement unit

Ideally there would be one multi-national global law enforcement unit dedicated to investigating child sexual abuse websites because the pace at which the trends[2] change are not conducive to traditional regional or national law enforcement and judicial structures.

5.4. Whilst there is, of course, agreement that children must be rescued from suffering and child sexual offenders must be investigated and prosecuted, the existence of different approaches to tackling this problem globally cause real challenges, including the fact that content remains available whilst an investigation is in progress. The 'potential' for every incidence of child sexual abuse content to be investigated (in a way that isn't implicit for other types of online content such as fraud) means offenders can themselves determine the speed at which to move their content before any serious investigative threat is posed.

5.5. In the UK, internet companies, government and police agree that content is captured and removed in the first instance regardless of impending investigation and that, where such removal cannot be quickly effected (for example, another country has no removal framework or wants it to remain available whilst they consider their investigative options) then that content should be blocked. Over 100 UK and international companies agree with such an approach by helping to fund the IWF's removal arrangements and over 60 companies now voluntarily subscribe to our block list. It is possible that effective global take-up of removal arrangements would in time make a block list increasingly obsolete although the speed of content movement means there may be a continuing role for access disruption for the short-term protection of users.

5.6. Phishing comparison

We know that some commentators believe that the speed at which phishing websites are taken down could be replicated in the case of child sexual abuse websites. However, this proposition overlooks a number of issues. Firstly, there is an implication that international private sector-facilitated removal of phishing websites has been effective in tackling the problem however this may not be the case. We understand in fact that phishing is on the increase therefore it is clear that a layered approach to such challenges, combining a number of tactics, is likely to be more effective than isolated removal. Furthermore there are a number of fundamental differences in the nature and severity of the content

[2] IWF opine that the commercial distribution of such content is not increasing but it remains a very serious challenge

concerned and therefore the likelihood is far higher that a law enforcement body would prioritise the investigation of the rape of a child than a phishing crime so they may be keen that such evidence does not disappear from the internet.

6. Tactical options

6.1. All the tactics below are carried out by the IWF in partnership with the internet industry and on a national and, where relevant, international basis, and could work effectively alongside an international law enforcement response.

i. National and or international **reporting mechanism** for the public to report (anonymously if they wish) their inadvertent exposure to child sexual abuse content.
ii. National and or international **reporting mechanism** for IT professionals to report their suspicions of child sexual abuse content on their networks.
iii. National and or international '**notice and takedown'** system to swiftly remove child sexual abuse content at source without compromising the simultaneous capture of evidence necessary to detect and prosecute offenders.
iv. Targeted assessment, monitoring and removal of individual newsgroup postings and **newsgroups** associated with child sexual abuse content.
v. Facilitation of network level URL-specific **blocking** to prevent accidental access to child sexual abuse content. As well as ISPs, a URL list can be deployed by mobile operators, search providers, content providers, filtering companies and other technology companies to help disrupt access.
vi. Working with domain name registries and registrars to **deregister domain names** dedicated to the distribution of child sexual abuse content
vii. Providing a list of **keywords** and phrases commonly used by those seeking out child sexual abuse content to companies to help prevent access to criminal content and the abuse of business networks and to help search providers improve the quality of search returns.

7. Network level blocking issues

7.1. Network level blocking has received attention from many quarters in recent years. The IWF has been providing a URL specific list to facilitate the blocking of child sexual abuse content[3] since 2004. This list is now deployed, on a voluntary basis, by over 60 companies across the UK and in many countries around the world including internet service providers, mobile operators, search providers and filtering companies. We are committed to sharing lessons we have learned in this area and we continue to refine our processes and policies to adapt to the changing nature of the distribution arrangements.

7.2. We take immediate action to effect the removal at source of child sexual abuse content hosted in the UK. If it is hosted abroad we pass details to our INHOPE Hotline partner or law enforcement colleagues in the hosting country so they can investigate the content in collaboration with the relevant national authorities and within their national legislation.

7.3. Whilst non-UK hosted child sexual abuse content remains live we add the URL to our list. Every URL on the list depicts indecent images of children, advertisements for, or links to such content. The size of the list fluctuates, averaging around 500 URLs at any one time, and is updated twice a day to ensure the list is comprehensive and the URLs are live. The URLs are assessed according to UK law, a process reinforced by reciprocal police training, with each image being categorised in line with published criteria set out by the UK Sentencing Guidelines Council.

[3] The list only contains child sexual abuse associated content.

8. Our points of view

i. We believe prompt removal at source is one key element to combating child sexual abuse images online and it is a function we facilitate on a national and increasingly international basis.

ii. Blocking is a disruption tactic which can help protect users from stumbling across these images whilst the relevant authorities investigate the distributors.

iii. Blocking can minimise the re-victimisation of the child by preventing images of their sexual abuse being repeatedly viewed.

iv. We support and facilitate URL-specific network level blocking as part of a range of tactics designed to disrupt the availability of child sexual abuse content.

v. Blocking cannot put an end to offenders abusing children nor can it deny determined criminals who are actively seeking such material.

vi. URL blocking does not deal with peer-to-peer exchanges.

vii. Network-level blocking of child sexual abuse content addresses a very specific kind of criminal content and does not guarantee a comprehensive safe online experience for family use. It should therefore be used in conjunction with safe search options, parental controls and supervision and or other end-user or client based filtering products.

viii. Some distributers of child sexual abuse content may have such resilient distribution networks or ‘business’ models that blocking and even removal will not seriously affect their activities in the long run nevertheless both tactics deny them stability to conduct their nefarious activities without fear of detection or disruption.

9. Trust and confidence in the IWF model

9.1. We provide advice, technical guidance, contractual arrangements, security, and self-regulatory standards to those companies who opt to take the URL list from us. Facilitating blocking through list provision is an important and trusted responsibility and our work is overseen by an independent Board according to approved policies and procedures, following legal advice and with the ongoing technical guidance of our industry members. Specialist police officers train our staff to assess content and we work within a strict legal framework. The systems and processes involved in handling reports, assessing content and compiling the list are also periodically inspected by a range of independent experts.

9.2. We should make it absolutely clear the IWF assesses criminal content only, we have no powers to investigate offenders but our existence in the UK adds value to UK policing because the majority of the 40,000 reports processed in 2009 relate to content hosted abroad and therefore outside the jurisdiction of the UK policing authorities. As we receive no funding from the UK government it follows that we do not benefit from funding intended for policing purposes.

10. Issues to consider when implementing blocking:

10.1. Collateral damage

It is our view that any list must be URL specific especially as much of the child sexual abuse content known to the IWF is currently hosted on legitimate internet services and so domain level blocking, DNS poisoning or IP address blackholing would make significant numbers of otherwise innocent internet services unavailable.

10.2. Regular updating

In our experience child sexual abuse content is highly transient and may move hosting company and country every few days. Therefore, to be as comprehensive as possible and to avoid the blocking of obsolete URLs or updated legal content any list should be refreshed and then redeployed at least once a day.

10.3. Location

Some internet locations which may be used for the distribution of child sexual abuse content are unsuitable for blocking therefore each instance of such content online needs to be considered on an individual basis for list suitability. Some examples include:

i. Blocking content on high-traffic websites might significantly reduce internet speeds for consumers.
ii. If the legitimate website deploys an intrusion detection system or its own censorship/vandalism policy then all visitors to the website could be blocked if the volume and nature of inbound traffic is not immediately recognised.
iii. Some private networks and encrypted traffic domains cannot be blocked on a page-specific basis.
iv. Highly dynamic image boards are also unsuitable for blocking because URL content changes rapidly as new posts are added.
v. Traffic managed via content delivery networks or with rapidly changing IP addresses may also be unsuitable for inclusion

10.4. Secure, confidential, contracted list provision

An effective list would include live hyperlinks leading to child sexual abuse content (and live advertisements linking to that content) so serious consideration must be given to whom and where that list is made available. It should only be provided across a highly secure interface. The processes and responsibilities undertaken by list recipients should be subject to confidentiality agreements, high levels of security and contractually protected. Access to any list should be controlled through a licence agreement to ensure details of deployment and liability for its (mis)use are formally agreed between all parties involved.

10.5. Transparency

Blocking should be carried out in a transparent way and, in the interests of wider public protection:

i. It is important that there is an easy way for the public to check which companies are blocking.
ii. Appropriate information should be displayed to a consumer when access to a page is denied.

10.6. Complaints and appeals process

A robust complaints and appeals process should exist to enable anyone with a legitimate association to the content to complain about its assessment and inclusion on a block list.

10.7. Quality of the List

Due to the potential for network level content blocking to be perceived as censorship, it is important to develop comprehensive ways to ensure the public’s trust and confidence in the list. In our opinion the credibility of the organisation providing the list is crucial. The organisation’s governance, oversight structures and the extent to which it subjects itself to public, independent and expert scrutiny are essential. Whilst it may be difficult or unfeasible (e.g. speed of movement of the content) for each URL to be inspected by the judiciary before inclusion on the list (we process approaching 40,000 reports a year and add 30-50 a day for example) it is important for an organisation like the IWF to display the highest standards of image assessment training, staff welfare, staff vetting, published threshold levels, process inspection, information security and reputational integrity in order to carry out such a job.

10.8. Scope creep

There is some concern that the infrastructures developed to facilitate the blocking of child sexual abuse content will be ab/used to block a wider range or criminal or even legal content in the future. Safeguards and commitments should be developed to ensure this concern is minimised and the specificity of the blocking (especially if it is mandated) is preserved.

10.9. Proportionality and cost

Considering the relatively small proportion of internet content that depicts child sexual abuse it is important that responses, particularly blocking, are proportionate and effectively balance online safety and protection with the right to freedom of information and cost of deploying blocking. It is our view that no-one should have a right to access child sexual abuse content therefore if blocking is done 'intelligently' then it could be a worthwhile addition to a range of tactics to disrupt access to the content.

10.10. Effectiveness of blocking

There is a dearth of evidence about the effectiveness of blocking. That is not to say that it is ineffective, however, the 'case for blocking' would be greatly enhanced if it could be independently demonstrated that access, supply, demand or volume of child sexual abuse content had been effectively reduced and images had been viewed less as a result. Some ISPs suggest, for example, that they are stopping tens of thousands of 'requests' for URLs on our list each day although it is not yet understood how many of these requests are from humans as opposed to internet spiders, robots, and so on. Similar work could be carried out in terms of the effectiveness of blocking by search providers, mobile operators and others. Indeed, anecdotal information implies that complicating access to this content may help prevent the curious from descending along a path of offending.

10.11. Verification of deployment and self certification

The provision of a list to a company does not help in determining whether that list is being deployed, whether it is being regularly updated and indeed whether it is preventing access to child sexual abuse content on the list and not to other legal content or legitimate services. Therefore, methods for certifying the effectiveness of list deployment by all relevant companies taking the list should be considered.

11.Looking forward

11.1. The longevity of some child sexual abuse content hosted outside the UK is still a major concern despite our promotion of 'notice and takedown' systems to remove it at source. Whilst acknowledging there are different approaches to managing this problem around the world we have been considering how we could have more of an impact in speeding up the removal of child sexual abuse content on an international basis without compromising any protocols between Hotlines and statutory authorities in various countries. We are working now to foster relationships with foreign internet service providers and hosting companies so that, in collaboration with their relevant national authorities, we can help more companies rid their networks of child sexual abuse content and reduce the length of time images remain available.

11.2. In response to changing criminal tactics in this area and new online services and technologies, we continue to refine our services and extend our reach as well as developing new initiatives to help our partners combat child sexual abuse content on their own systems and across the internet as a whole.

12.Contact

If you are interested to discuss any of the issues raised in this paper please contact the IWF on +44 (0)1223 237700 or email admin@iwf.org.uk. For more information on the IWF, see www.iwf.org.uk.