1 A Brief History of Child Safety Online: Child Abuse Images on the Internet

John Carr

COPYRIGHTED MATERIAL

Foreign holidays used to be a rare treat enjoyed by better-off families, but otherwise, until the Internet arrived, the great majority of the world's children and young people spent pretty much their entire day-to-day lives exposed to and governed by the mores, sights, sounds and laws of one country, usually the one where they were born and lived. The opportunities open to children and young people, as well as any threats or dangers they might encounter on their pathway to adulthood, were generally well understood by their parents and their communities, because more or less everyone had lived through similar situations themselves. The Internet[1] changed that. A great many parents and the social institutions charged with safeguarding children were overtaken by events, and it is still by no means clear when or even if a new equilibrium will be established.

UNINTENDED, UNFORESEEN AND UNWANTED CONSEQUENCES

None of the scientists and technologists involved in the early development of the Internet had any idea it would turn out the way it did. Thus in many ways what the world is now having to grapple with in relation to online child abuse images as well as several other areas of crime is an example of the doctrine of unintended, unforeseen and definitely unwanted consequences being played out on an epic scale.

Without computers there could be no Internet. It is therefore tempting to begin a discussion of the history of the Internet by looking first at the history of computing and tracing the journey from there. However, according to the

Online Risk to Children: Impact, Protection and Prevention, First Edition.
Edited by Jon Brown.
© 2017 John Wiley & Sons, Ltd. Published 2017 by John Wiley & Sons, Ltd.

Internet Society[2] the real Internet story does not begin until the 1960s with the development of packet switching and later the ARPANET.

In February 2013, in a famous TED Talk,[3] Internet pioneer Danny Hillis describes the Internet as it was in 1982: '... it was a very small community. We didn't all know each other but we all kinda trusted each other . . .'

For many years, almost by definition, every Internet user was a highly educated adult. There was a great deal of reciprocity involved in running the network – everybody had a more or less equal stake in its continuing success. Users would behave responsibly within a framework of commonly accepted if typically unstated norms.

During his TED Talk Hillis brandishes in his hands a slender volume that contained the names, email addresses and telephone numbers of everyone who had an Internet account in 1982. He suggested that today a similar volume, if it could be constructed at all, would be about 25 miles high.

In short the early developers of the Internet, although they had a good idea about its potential to do good in the world by facilitating rapid communications between researchers and later businesses, they had no idea that what they were building would end up being exploited on a large scale by criminals to make or distribute child abuse images or to engage in any other type of felonious activity. If they had there seems little doubt they would have built in more security protocols to inhibit such antisocial behaviour.

SEXUAL IMAGES OF CHILDREN

Today child abuse images are very heavily identified with the Internet, but nobody would ever seriously argue the Internet is truly a *cause* of children being abused or of images of that abuse being made and distributed. The Internet has certainly opened up pathways that, for practical purposes, never previously existed, but that is a different point albeit one of some importance.

The development of photography and printing techniques in the 19th century first allowed for the larger-scale production and distribution of pornography of every type, including some depicting child sex abuse. However, as far as we can tell, since time immemorial there seems always to have been a small but still numerous minority of people,[4] mainly but by no means exclusively men, who have had an interest in children as objects of sexual desire or in depictions of children engaged in sexual acts.

In the UK in 1986, before the mass Internet emerged, one of the world's top paediatric specialists, Professor Oliver Brooke, was sent to prison after admitting dealing in and collecting child pornography. When police searched his office at St George's Hospital in London, they found more than 300 photographs of children in explicit sexual poses, 22 albums of cuttings from child pornography magazines and a dozen Danish magazines specialising in child pornography. Professor Brooke, who was later barred by the British General

Medical Council from ever practising again as a doctor, was at the time considered to be one of the five top specialists in the world in his field.

Also in 1986 a British local government surveyor, Charles Norris, was sent to prison for sexually abusing young boys and making indecent images of children. Police discovered 5,500 colour slides, 3,500 photographs, 29 photograph albums, 100 videos and 200 books and magazines – mainly featuring young boys – at his home in Kent. Again, Brooke had no connection to the Internet.

Nevertheless, with a limited number of exceptions[5] in modern times any sort of sexual interest in children and depictions of it have been the subject of severe societal disapproval based on an appreciation of the harm done to children by early sexual encounters with adults or by other forms of premature involvement with sex.

The law has intervened to underpin, reinforce and reflect these societal values. For example in all major jurisdictions around the world the possession, production and distribution of images of children engaged in sexual acts is now a criminal offence[6] and the age at which it becomes lawful for someone to be depicted in a published sexual image is not necessarily the same as the age of consent to sex.[7]

In 1995, on the eve of the Internet explosion in the UK, the police in Greater Manchester recorded the seizure of only 12 child abuse images in the entire year. In 1995 UK police as a whole were said to have known of the existence of only 7,000 unique child abuse images. INTERPOL then had records of only 4,000 known unique images.

In 'People Like Us,' commissioned in 1996 and published in 1997, Sir William Utting described the production and distribution of child abuse images as being a 'cottage industry.' That was probably about the last moment a statement like that could have been made.

What Sir William meant was that, traditionally, people who wanted to get hold of child abuse materials had to find or know a person who already had some. Alternatively they would need to take considerable personal risks to locate a stranger who could and would oblige or risk asking someone to send them material through the post. With the Internet, a few mouse clicks could put them in touch with a supplier who could deliver in an instant and on a completely unprecedented scale.

THE WORLD WIDE WEB EXPLOSION

At the end of 1980s and at the beginning of the 1990s the Internet was still nothing like it is today. The World Wide Web and the web browsers that would provide easy access to it were just around the corner.

Web browsers did for the Internet what Windows has done for personal computing: made it accessible to the non-technical masses. As with Windows, browsers deployed a 'graphical user interface,' using *intuitive* icons. These enabled people who did not have a degree in computer science or perhaps a

great deal of patience to carry out what would otherwise be quite complex operations potentially involving dozens of obscure, hard-to-remember keystrokes. All they had to do now was click on a little picture.

The first web browser famously was developed at CERN in Switzerland by Tim Berners Lee in 1989–1990. In 1993 the first publicly available web browser arrived. It was called 'Mosaic,' followed in 1994 by 'Netscape,' then in 1995 came Microsoft's 'Internet Explorer.' This was given away free and would go on to capture, at its height, over 95% of the entire web browser market.

Louis XV of France died in 1785, but not before uttering the immortal words '*Apres moi le deluge*' (After me, the deluge). Four years later the French Revolution began. The arrival of the web browser was a revolutionary moment of a different kind. Web browsers opened up the Internet to the rough, rude and larger world that hitherto had been excluded from its gentle cloisters.

AFFORDABILITY, ACCESSIBILITY AND ANONYMITY – *THE THREE As* – PROVIDE THE SPUR

The arrival of the web coincided with a fall in hardware prices, a fall in telecommunications costs and an increase in connection speeds. Affordability and accessibility were here. The belief in anonymity would come soon and complete the circle.

As noted, Sir William Utting had observed that prior to the arrival of the Internet the production and dissemination of child abuse images were essentially local and small scale. If there were larger numbers of people who were interested in child abuse images they seemed to be unwilling to take the risks associated with obtaining them or were disinclined to go to the trouble. The Internet was cheap, easy to use from the comfort of one's own home and it was being widely reported in the press that it could be used anonymously. It opened doors many were to go through who very likely would not have done so otherwise, and it is clear many did because they thought they would be anonymous.

However, the anonymity proffered or suggested in those early days was a false promise, which can largely be laid at the door of inaccurate reporting in the mass media. It was to cost a number of men their lives.[8] When they were eventually caught and arrested for child abuse image offences, a number of downloaders chose to commit suicide rather than face the humiliation of a public trial. For that reason today in the UK anyone arrested for this type of offence is usually put on 'suicide watch' or given some other form of support.

In the beginning it appears people would log on to different parts of the Internet or use their credit card to buy illicit items seemingly believing they had been rendered invisible. Even today some of the individuals who still go online looking for child abuse images apparently believe they are protected by anonymity, but such has been the publicity about so many cases that only the naïve, the foolish or the reckless can now labour under this kind of misapprehension.

The truth is it is almost impossible to go online without leaving some sort of footprint. The only question that matters therefore is whether or not your case will become one that the police choose to investigate. Such are the volumes in many countries there might have to be something exceptional or unusual about you or your case for it to rise to the top of the pile, and the worry is many criminals now know this.

More shocking still, perhaps, the world discovered that the Internet was also enabling like-minded people to find each other in ways that were simply impossible or impractical before. People with a sexual interest in children or an interest in child abuse images started to form groups, sometimes quite large with hundreds of members, dedicated solely to the production, distribution or exchange of child abuse images.

Groups were forming online in which participants would swap advice and give each other tips about how to find children to abuse and how to do it with minimal risk of being caught or successfully prosecuted. Some of this abuse would result in new images being made and distributed; some of it would not. By and large, though, the people in these groups would never have met in real life and probably never could have done so because they were scattered all over the planet.

Worse, these groups in effect became communities. They would reinforce and 'normalise' the behaviour of everyone in the group. Someone who had probably always thought of himself as being a bit of an oddball, who knew he had to keep quiet about his sexual preferences or interests and watch his behaviour generally, was now in touch with people just like himself. Maybe he started thinking he wasn't so strange after all. Maybe his tastes weren't that peculiar. When everyone else was being so censorious about the sort of sexual images he was interested in he could convince himself they had just got it wrong or hadn't yet realised what they were missing.

A *Panorama* programme broadcast by the BBC[9] in 2001 showed an interview with a man (David Hines) who, during Operation Cathedral, was arrested for possessing child abuse images that he had downloaded from the Internet or had been sent to him by people with whom he was in touch. In the TV interview Hines said, 'Thanks to the Internet, for the first time in my life I had friends. I had friends all over the world.'

THE NUMBER OF ARRESTS AND POLICE OPERATIONS START TO CLIMB

In 1988 the total number of people found guilty in Magistrates' Courts for child abuse image–related offences in England and Wales was 33. By 1992 it had grown to 72 and by 1995, arguably the Internet's year 0 in the UK, it had increased to 91.[10] The trajectory was moving in only one direction. It rose to 340 in 2001 and, when Operation Ore later got underway, the yearly numbers

exceeded or were about 1,700. They settled back to a 'normal' level in excess of 1,000 before rising again to about 3,000.

The other feature of this growth in the number of arrests was the numbers of images being seized by police. As previously noted, during pre-Internet times, typically an arrest might lead to the confiscation of a handful or a few hundred pictures, or as in cases such as Brooks and Norris, thousands. In the digital world a great many seizures would be counted in the tens if not hundreds of thousands and, not infrequently, in millions, although here there would be vast number of repeats of the same images. Following a Freedom of Information request made by the NSPCC it emerged that in England and Wales, within a two-year period ended in March 2012, five local forces had seized a total of 26 million images. If extrapolated to the whole of England and Wales, this suggests that in excess of 300 million images may have been in circulation during the same two-year period. Moreover it emerged that the police had identified between 50,000 and 60,000 individuals across the UK as a whole who had engaged with illegal child abuse images online, and in 2016 this number was revised upwards to 100,000.[11] When set against the police's historic record of arrests for these types of crime (see the previous paragraph) a very depressing picture emerges that underlines how unlikely it is that this type of crime will ever be satisfactorily addressed via traditional or conventional law enforcement methods. And the key point to grasp here is that although these numbers are very obviously derived from a single country, the UK, there is absolutely no reason at all to believe that the situation will be significantly different in any other jurisdiction where similar levels of Internet access and access speeds exist.

By the mid-1990s it was clear that 'something had to be done' about this 'new-fangled' and still uncertain technology called *the Internet* and the evil that seemed to be arriving in its wake. But what? There were no textbooks to guide anybody. One of the solutions that people eventually came up with was Internet hotlines. These were places where members of the public, employees of Internet service providers or indeed anyone, could report any child abuse images they had seen online, in anticipation of them being investigated and removed as soon as possible. At that time there was a widespread consensus that the scale of the problem was such that finding ways of involving the public in the fight against these images was an essential component.

The UK, Norway and Holland were the first in the field. In each country the pressures were the same but the organisational arrangements turned out differently. Here we look in a little more detail at how the UK's hotline emerged.

THE EMERGENCE OF HOTLINES

In the early 1990s a steady stream of stories of arrests for child pornography offences started to reach the UK media. They received huge coverage in the press. Partly this was a reflection of the fascination by journalists and their

readers, viewers and listeners with an awesome new technology. Partly it was a reflection of a natural if somewhat ghoulish curiosity in something so viscerally awful. Elements of the Internet industry complained loudly about how unfairly they were being treated by the media, but in a democracy where a free press is highly valued, the sort of coverage the stories were given was 100% predictable and 100% inevitable. It was no use crying 'foul.'

Although there was a lot of development going on in the background, from the public's point of view the UK's Internet industry then consisted principally of a small number of Internet service providers (ISPs) who were delivering Internet connectivity to people's homes. The largest of these was BT.

Perhaps the real problem was that the fledgling industry was unable to promote or establish in the public's mind an alternative explanation, a better or more convincing, reassuring narrative that would put into perspective or explain how it was that their new systems were suddenly facilitating such appalling behaviour.

Eventually, in 1995, an industry trade association would form – Internet Services Providers' Association (ISPA) – to act as an intermediary and spokesperson for the industry, but they still found themselves overwhelmed and drowned out by the noise and anger that child abuse images seemed to create whenever the issue was discussed in public.

Some newspapers and TV or radio stations undoubtedly did occasionally overstate or sensationalise aspects of police operations in this space. This certainly increased the pressure on the police and politicians to be seen to act. But none of the media outlets was making it all up. There was a lot of smoke, but there was plenty of fire creating it.

Opinion polls started showing high levels of anxiety among parents about the threat to children that the Internet seemed to represent, much of it triggered by stories about child abuse images, although this was added to considerably when stories about the easy accessibility of legal adult pornography and other materials not suitable for children started to appear.

MPs were hearing about these issues on the doorstep, in letters from constituents and at their surgeries. Politicians were becoming convinced that they had to act but there was no clear idea about what they should do. Lead responsibility for this area of policy within government lay with the (then) Department of Trade Industry (DTI) who, broadly speaking, saw their job as helping the Internet in the UK to grow as quickly as possible. They did not see themselves as being in the business of promoting any kind of restrictions for fear this might kill off the goose that everyone hoped was going to lay the golden egg of new kinds of economic growth.

But who was responsible and for what exactly? There seemed to be little technical understanding of how the Internet operated among the UK's police forces and even less among the crime correspondents of the major media outlets.

Despite some wild assertions to the contrary that surfaced from time to time nobody seriously believed the owners or employees of any of the UK's ISPs

were intentionally or knowingly causing or allowing illegal images to be stored or distributed through their systems. Thus the element of intentionality, essential for almost every major crime, was simply not there. Absent such intentionality, how far was it reasonable to go to expect the people who were developing the exciting new Internet industry in Britain to step in and deal with the problem, and just what did 'dealing with the problem' mean in practical terms?

Media stories were starting to reach the UK from overseas, in particular from France and Hong Kong. The police there were being very muscular and direct in their dealings with their local ISPs. They were reported simply to have walked on to the ISPs' premises, unplugged the servers and took them away, arresting and detaining for questioning any directors or senior employees they could find. They did not sit about and engage in philosophical debates about culpability, causation and intentionality. Their simple view was the images were coming off or being distributed from their machines so they must be responsible. The British media noted this with approval. They wanted some of it here. Pressure was mounting.

Events began to move rapidly in the summer of 1996.

THE BIRTH OF THE INTERNET WATCH FOUNDATION

The Internet Watch Foundation (IWF) owes its immediate existence principally to three far-sighted men. One was Chief Inspector Stephen French of the Metropolitan Police's Clubs and Vice Unit. The second was Ian Taylor, MP, Minister for Technology at the DTI, in John Major's Conservative Government. The third was Peter Dawe, founder of Pipex, one of the UK's first commercial ISPs. Dawe sold Pipex for a very large sum of money and became extremely rich. This meant he could do things that others could not. Dawe did not have to convince a committee or anyone else to put up money for this or that idea. He decided for himself.

First step forward Chief Inspector Stephen French. In August 1996 he sent his famous open letter to ISPA and to several of the larger ISPs. He said the police had identified more than 130 Usenet Newsgroups[12] that they believed contained illegal material and that the police's view, in essence, was that the ISPs were in effect the publishers of it. The police wanted the named groups to be banned.

The key part of his letter said

> 'This list is not exhaustive and we are looking to you to monitor your newsgroups identifying and taking necessary action against those others found to contain such material. As you will be aware the publication of obscene articles is an offence. This list is only the starting point and we hope, with the co-operation and assistance of the industry and your trade organisations, to be moving quickly towards the eradication of this type of newsgroup from the Internet . . . We are very anxious that all service providers should be taking positive action now,

whether or not they are members of a trade association. We trust that with your co-operation and self-regulation it will not be necessary for us to move to an enforcement policy.'

This was not a very thinly veiled threat, although in truth the police and the Crown Prosecution Service were not at all sure what the basis for any arrests might be. Here is where the government came in through Ian Taylor. Taylor made it clear that if the industry did not sort things out via a self-regulatory initiative of some sort there would be legislation to create arrestable offences.

There had already been something of precedent for self-regulation in the Internet space in Britain. In May 1996 it had been agreed that Nominet would be established as a self-regulatory body to take over the complex task of administering the .uk domain space.

The Observer ran a major story that honed in on the distribution of child abuse images by British ISPs.[13] It became crystal clear to the Internet industry that this issue was not going to go away any time soon. In September 1996 Dawe got enough people from the industry around the table to sign up to a new body that initially was to be called the 'Safety Net Foundation' but would finally become the IWF. Its role was to receive reports of child abuse images that were found on the Internet and to secure their removal as rapidly as possible by issuing a notice to the hosting company that, in practice (though not in theory), required them to remove the image forthwith.

However, there was never any serious suggestion that the businessmen and - women who had formed the UK's first ISPs knew or could know who was posting illegal material to their servers or where it was being kept. What was being expressed by the media and politicians was a *cri de coeur* (cry of the heart). What the police and others were looking for was help to deal with some of the nastier consequences of the rollout of the technology from which the ISP shareholders hoped to profit. The police and government wanted industry to show it felt some sense of responsibility, of ownership.

Fortunately, wise counsels prevailed. Big companies such as BT and several others saw that what Peter Dawe was saying was right anyway, whether or not it got them a get-out-of-jail card. They didn't want those sorts of images circulating on their networks. They did not want to be thought of as 'child porn merchants.' They recognised the need to create new machinery to help them identify the illegal pictures and inform them of their whereabouts, so they could remove them as rapidly as possible.

The fact that BT came out in this way was highly significant. It was also a harbinger. The plain truth is that as more and more bigger businesses started to get involved in the Internet attitudes started to change, or to put it more bluntly, a division opened up which more or less corresponded with the size of the firm. The bigger the company the more it was accustomed to working in the consumer space. Larger firms were already on the High Street, metaphorically and in some cases also literally. These firms had no difficulty grasping the importance of being seen to deal vigorously with an issue such as child abuse images.

Admittedly these larger companies were likely to be more highly capitalised than their smaller rivals and therefore were better able to cope with changing or new demands, all of which cost money and could consume valuable engineering time with perhaps little to show for it on the bottom line in the short run.

Internet self-regulation as an official policy in the UK for dealing with child abuse images therefore grew out of necessity and the exigencies of the moment. It started with a letter from a policeman. Self-regulation was not a carefully selected option picked from a range of possible choices. Civil servants in the Home Office or elsewhere with any sort of background in how the Internet worked were somewhere between thin on the ground and non-existent. Presumably there were people in the security services who were on the case but they weren't much in evidence near Westminster and Whitehall at the time.

Aside from Chief Inspector French and a small number of his colleagues in the Metropolitan Police, almost nobody in mainstream law enforcement then knew anything about the Internet. The National Criminal Intelligence Service was taking a leadership role but, at the operational end, the National Hi Tech Crime Unit would not be established until 2001. The police and the government were just relieved that the IWF came along to take the strain.

One of the major and continuing unsung benefits of the IWF and other hotlines around the world is how much it saves in police time and hence taxpayer money. About two-thirds of all the reports the IWF receives concern images or things that are not illegal but the person reporting them thought they should be. The IWF in effect acts as a filter.

As already noted for many years the lead department for anything and everything to do with the Internet was the DTI, thus emphasising the focus of government policy back then. Even the Internet Crime Forum was run under the DTI's umbrella. The first written communication between the UK's children's charities and the UK government on anything to do with the Internet was in March 2000, and it was in the form of a letter to Patricia Hewitt, MP at the time Minister for Small Business and E-Commerce. It would be a while before the Home Office and what would become the Ministry of Justice became fully engaged.

What was happening in the UK was also happening everywhere else in the developed world. A paper discussing the role that hotlines could play in a campaign to eradicate online child abuse images was presented to the 1st World Congress Against Commercial Sexual Exploitation of Children, held in Stockholm in August 1996. The paper had been written and presented by Save the Children Norway and the Norwegian Children's Ombudsman, but the Norwegian hotline did not actually begin operations until January 1997. To begin with and for several years, Save the Children, Norway, managed the hotline, working closely with the Norwegian police.

As a percentage of the total population of Internet users worldwide and in absolute numbers, in the beginning the largest concentration of Internet

account holders was in the United States, home of the Internet. Even so the United States did not establish a hotline until 1998 when the National Center for Missing and Exploited Children created their Cyber Tip Line.

In Holland the prime movers seemed to be the Internet industry. In Norway it was a children's organisation. As we have seen in the UK it was the police and the government that encouraged the industry to act, and the IWF, an NGO, was the result. Similar coalitions started to be formed in many parts of the developed world although in some, for example, Australia, it was the state that directly initiated the hotline.

INHOPE, a global association of hotlines, was established in 1999 and today has 54 member hotlines in 45 countries. That means there are more than 150 countries in membership of the United Nations that do not have a hotline, although some of these are very small and have not featured as major hosts of child abuse materials, at least not yet. Alternatively members of the public have to report via the police.

INHOPE has recently established a charitable foundation with the express aim of helping countries in the developing world to create operational hotlines. The IWF has also developed a package that is thought to be particularly suitable for smaller countries where hosting illegal images is not an issue but where, nonetheless, the public still want to be able to report illegal content to a site that is locally based and in their own language.

More worryingly there are still a substantial number of countries around the world that still do not have an adequate legal framework to deal with online child abuse images. Published in 2016, the eighth edition of the International Centre for Missing & Exploited Children's global review[14] indicated that there were still 50 mainly smaller countries in the world where simple possession of child abuse images is still not illegal.

NOT A VERY PROMISING START

At the beginning of the IWF's operations the main focus was Usenet Newsgroups. Chief Inspector French's letter referred only to Newsgroups. The rule established early on was that the IWF staff members had no power or authority to go looking for child abuse material on the Internet. They had to wait for a report to come in, and then they had to deal with each report individually.

This idea of only reacting to reports received is still very common in the Internet space but, at root, it is in many ways a rather curious proposition. If someone goes online looking for material they are interested in and they find it they are hardly going to report it if that might lead to it being removed from the Internet altogether. This is even more the case when the material in question is itself illegal, and it is also a crime to seek it out intentionally.

The IWF used to have several people who regularly reported material to them and staff members were obliged to point out that, however noble their intentions might be, if they were deliberately seeking out child abuse images they would in

fact be breaking the law. The worry was such individuals might be trying to establish an alibi or a plea in mitigation when in truth they were simply collecting child abuse images for their own consumption. Thus the whole basis on which the IWF was established relied on people reporting material they had found accidentally or that had arrived in their in-box unsolicited.

Thus, under the originally agreed processes within the IWF if someone posted a photograph with a caption that informed the viewer it was a 'picture of a baby being raped' in a Newsgroup that might be called 'Pictures of Babies Being Raped' all the IWF staff members could do was confirm that the image was illegal and issue a notice the effect of which would be to get that specific posting taken down. It could be back up again within minutes, in exactly the same Newsgroup, yet the staff members were powerless to act until a further complaint was received. Similar procedures were in place in other hotlines in other countries.

The system was seen by some in the UK as being absurd; moreover, a little legal research led to the discovery that the Protection of Children Act 1978, specifically s.1 (1) (d), says it is an offence for a person

> 'to publish or cause to be published any advertisement likely to be understood as conveying that the advertiser distributes or shows . . . indecent photographs or pseudo-photographs of children or intends to do so.'

Was a Newsgroup name an advertisement? The question was not definitively answered until July 2002 when barrister Anthony Hudson replied in the affirmative. Meanwhile what about those Newsgroups that, whatever their name, regularly had child abuse images posted to them?

In early 2001 it was suggested the IWF embark on a new policy of banning entire groups that appeared to advertise the availability of child abuse images and groups that regularly contained such images irrespective of its individual name. Eventually this policy was agreed on, even though it was anathema to the then-traditions of the internet.

The monumental nature of this decision cannot be overstated. If the decision on Newsgroups had gone the other way, it is inconceivable that the IWF and BT would later have felt there was any point in co-operating in the experiment that lead to the announcement of *Cleanfeed* in June 2004[15] (see more in the next section), a world first that is now emulated across the planet.

THE TERRAIN SHIFTS AND URL BLOCKING EMERGES

In the early part of the 21st century, child abuse images started popping up on websites with greater frequency. The web was a completely different environment from Newsgroups. The problem was that, overwhelmingly, the images

being reported were hosted outside of the UK. It could sometimes take weeks, months, even years for them to be removed.

The unconscionable delays in take-down times were very effectively exposed in a study published by Richard Clayton and Tyler Moore of Cambridge University.[16] They contrasted the average speed with which phishing sites could be removed – hours – with the length of time it took child abuse images to be removed. Their explanation was simple and devastating. Phishing sites could cost the banks money. The banks were on the case. There was no comparable system of incentives that worked in relation to child abuse images.

The delays in pictures being taken down meant two things. First was the implication that the image was being ignored or not dealt with promptly by the local police in whatever country it had ended up. This meant no one could have any confidence that serious efforts were being made to locate the children and rescue them from whatever catastrophic situation they must be in for the events shown in the images to be possible in the first place.

Second, for as long as the images stayed up on the website they remained visible within the UK. For that reason their continuing publication further violated the rights of the child or children depicted in them and could put them in danger of being abused again; to the extent that their continued visibility and availability for download encouraged or sustained paedophile activity within the UK, they represented a continuing threat to children living in the UK.

Following the decision on Newsgroups the UK government became convinced that a similar approach might be tried in relation to the web. Nonetheless this time around, when thinking about how to deal with the web, in 2003 the Home Office decided to convene a working group of ISPs to discuss the technical feasibility of blocking web addresses.

There was considerable opposition from most of the ISPs on the working group to the idea of attempting to block web addresses. To their eternal credit BT said they were willing to try to build and test a URL-blocking system if the IWF would agree to give them a list of URLs. The IWF did. Officers of the Metropolitan Police were also on the working group. They indicated that they had no objection to such an experiment being carried out but, unlike their earlier intervention in Newsgroups in 1996, they were not the prime movers on this occasion.

Out of this BT developed *Cleanfeed,* which, as noted, came blinking into the world in June 2004. Once it became established in the public domain that blocking was technically feasible and was in fact happening, the need for the Home Office working group disappeared. It never met again.

Today almost 100% of domestic broadband users in the UK now belong to ISPs that deploy the IWF list. Every mobile phone network deploys it, and all of the major WiFi providers in the UK also use it on their networks. It is also used by all the major search engines. There is no question that this BT-IWF

initiative was hugely important, and now very many countries around the world are emulating it. In Italy URL blocking is required by law. Blocking even found its way into an EU Directive on Child Protection in 2011.

TECHNOLOGY COMES TO THE RESCUE OF A PROBLEM TECHNOLOGY HELPED TO CREATE

As we have seen, law enforcement agencies no longer have the resources to investigate every case in which someone is suspected of being engaged in the distribution or downloading of child abuse images.

The first attempts to use technological solutions to reduce or eliminate the traffic in images started to be deployed with the emergence of hotlines that arranged for the images to be removed from the Internet, then largely within Usenet Newsgroups. Later this evolved in the UK and a growing number of countries into the use of blocking lists of URLs known to contain illegal images or to restricting access to certain Usenet Newsgroups. Yet the volumes continued to grow. The emergence of social media sites and file locker services[17] also presented a vastly increased number of opportunities to persons with an interest in these images to store and distribute them. New solutions were needed.

Although for some time a number of smaller companies had been working on technical solutions that would enable known illegal images to be identified, no major technology players were known to be engaging with the challenge. Many saw this as a law enforcement problem not a business opportunity. Microsoft was the first big player to step forward. In 2009 the company announced that it had been working with technologists at Dartmouth College to develop PhotoDNA. Microsoft describe PhotoDNA as 'an image-matching technology . . . It creates a unique signature for a digital image, something like a fingerprint, which can be compared with the signatures of other images to find copies of that image. NCMEC and online service providers such as Microsoft and Facebook currently use PhotoDNA to help find, report and eliminate some of the worst known images of child pornography online, helping identify thousands of these horrific images that would previously have gone undetected.'

These unique fingerprints are more commonly referred to as 'hashes,' and law enforcement agencies and companies around the world are pooling their hashes and allowing them to be assembled into large databases that can then be used to identify matching images. This can help save an enormous amount of time and effort of the part of the police, who will no longer find they are investigating an image that has already been dealt with by a police force in another country. Google, Twitter and many other companies are now using PhotoDNA, and the hope must be that every company that operates online will do so.

The main drawback with PhotoDNA is that it works only with still images. It does not work with video footage of which there is now a huge quantity online. Google has stepped into the breach to try to solve this problem with a programme that works with video clips in a similar way to PhotoDNA and stills. In late 2016 the Canadian hotline started using a hash database with very impressive results.[18]

THE ROLE OF SEARCH ENGINES

In the aftermath of the trials for the murders of April Jones and Tia Sharp in 2012 a great deal of attention fell on the role of search engines in helping paedophiles to locate child abuse material on the Internet. This was to have global consequences. Google and Microsoft said they were going to make changes to the way in which their search engines operated, making it harder for anyone to locate paedophilic content. They also indicated their intention to introduce *splash pages*. Thus in future if people used either search engine to attempt to find paedophilic material a message would appear on the search page warning them that they were likely committing a criminal offence and also pointing them towards potential sources of help if they were worried about their behaviour. Both companies said they were going to roll out this new approach in every language and territory in which they operate. Precise information on the progress being made in delivering on these promises and on the impact of these measures has yet to be made publicly available by either company.

THE UNANSWERED QUESTIONS ABOUT TECHNICAL SOLUTIONS

In some quarters there is undoubtedly a degree of ambivalence about the idea of looking to technology to solve the problems presented by the extremely large quantities of child abuse images being circulated on the Internet. Undoubtedly some would rather we simply increased the number of police officers employed in this work so that anyone who engaged with the images might, as a result, reasonably fear that sooner rather than later there would be a knock on their door following which they would be arrested then later convicted.

It is sometimes pointed out that a significant proportion of those who *are* picked up following an online investigation into child abuse images have not previously been known to the police or other authorities; consequently, the Internet is presenting an unprecedented opportunity to uncover potential or actual child abusers in ways that otherwise do not exist. In the end this argument is circular and self-serving. It is a bit like arguing law enforcement should tolerate the continued distribution of drugs in order to follow the trail to

discover who the drug addicts are. Implicit in this line of thinking is also the suggestion that the right to privacy and human dignity of the victims depicted in the images counts for a great deal less than it should. Moreover it is important to remember it is not just the numbers of trained police officers that count here. With an increased number of arrests for image-related offences would also come an increase in the demand for forensic examinations of seized equipment, an increase in the demand for staff members capable of carrying out psychological or other assessments of those arrested, an increase in probation and prison staff members, possibly also an expansion in the number of prison places, not to mention an increase in the number of court rooms, judges, lawyers and associated staff members to make all this work. It is doubtful, in the midst of a global recession and times of austerity, whether it is realistic to expect countries even in the richer parts of the world to be able to contemplate the sorts of expansion in public expenditure such an approach suggests, and it is surely completely unrealistic to expect less prosperous parts of the globe to be able to do likewise.

Naturally everybody would much rather find effective ways to prevent any kind of child abuse from happening in the first place but, absent that, dealing with images of it, without more resources, is a vitally important policy goal in its own right. Dealing with illegal images of children with the current level of resources should never be considered secondary to or of less importance than other important policy objectives in this space. There is no hierarchy of need or importance. Each aspect requires specific approaches. Neither should they be seen as being in competition with each other.

NOTES

1 There are now a wide range of devices that can connect to the Internet, many of them highly portable and used by children and young people on a large scale, for example, smartphones, tablets and games consoles. All references to the Internet encompass the use of any and all of these, although the degree of risk associated with any particular method of connecting can vary by degrees.

2 Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., & Wolff, S. (2016). *A brief history of the internet*. Internet Society. Retrieved February 14, 2017, from www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

3 Danny Hillis: The internet could crash. We need a plan b. *TED Talk*. Retrieved February 14, 2017, from www.bing.com/videos/search?q=Danny+Hillis+TEDTALK&view=detail&mid=6E28E5B88111C9A59CF46E28E5B88111C9A59CF4&FORM=VIRE

4 Stephenson, W. (July 30, 2004). How many men are paedophiles? *BBC News*. Retrieved February 14, 2017, from www.bbc.co.uk/news/magazine-28526106; see for a summary of Michael Seto's views.

5 In some Scandinavian countries for a brief period in the 1960s child pornography and sexual acts between adults and children were not illegal.
6 International Centre for Missing & Exploited Children. (2016). *Child pornography: Model legislation & global review* (8th ed.). Retrieved February 14, 2017, from www.icmec.org/wp-content/uploads/2016/02/Child-Pornography-Model-Law-8th-Ed-Final-linked.pdf. But note (page 10) 50 countries still do not outlaw simple possession.
7 Child Exploitation and Online Protection Centre. (June 2012). *A picture of abuse: A thematic assessment of the risk of contact child sexual abuse posed by those who possess indecent images of children* [Executive summary] (p. 4). Retrieved February 14, 2017, from www.ceop.police.uk/Documents/ceopdocs/CEOP%20IIOCTA%20Executive%20Summary.pdf
8 Tendler, S., & Searle, D. (January 11, 2005). Operation Ore link in suicide of navy chief. *The Times*. Retrieved February 14, 2017, from www.thetimes.co.uk/tto/news/uk/article1921242.ece
9 Wonderland Club paedophile ring (Operation Cathedral). *BBC News*. Retrieved February 14, 2017, from www.youtube.com/watch?v=iHAgCQdvw94
10 Offending and Criminal Justice Group (RDS), Home Office Ref: IOS 503–03.
11 Gallagher, P. (October 13, 2016). Number of people accessing child abuse images feared to have doubled in three years. *News: The Essential Daily Briefing*. Retrieved February 14, 2017, from https://inews.co.uk/essentials/news/health/thousands-seek-help-child-abuse-images-online/
12 McKay, N. (August 22, 1996). British police list 133 obscene newsgroups. *Computerworld*. Retrieved from www.computerworld.co.nz/article/519610/british_police_list_133_obscene_newsgroups/
13 Connett, D., & Henley, J. (August 25, 1996). These men are not paedophiles: They are the internet abusers. *The Observer*.
14 International Centre for Missing & Exploited Children. (2016).
15 Blight, M. (June 6, 2004). BT puts block on child porn sites. *The Guardian*. Retrieved February 14, 2017, from www.theguardian.com/technology/2004/jun/06/childrens services.childprotection
16 Moore, T., & Clayton, R. The impact of incentives on notice and take-down. *Seventh Workshop on the Economics of Information Security* (WEIS 2008), June 25–28, 2008. Retrieved February 14, 2017, from www.cl.cam.ac.uk/~rnc1/takedown.pdf
17 Cyberlocker. *Techopedia*. Retrieved February 14, 2017, from www.techopedia.com/definition/27694/cyberlocker
18 A game changer? (January 26, 2017). *Desiderata*. Retrieved February 14, 2017, from https://johnc1912.wordpress.com/2017/01/26/a-game-changer/