2012

Online Child Protection

Commonwealth IGF

Commonwealth Internet Governance Forum

A Joint Report on

Online Child Protection
Combatting Child Pornography on the Internet

from
the Children's Charities' Coalition on Internet Safety
and
the International Centre for Missing and Exploited Children

by
John Carr

A publication of
The Koons Family Institute on International Law & Policy,
an initiative of the
International Centre
FOR MISSING & EXPLOITED CHILDREN

Foreword

The Commonwealth Internet Governance Forum (CIGF) is a virtual space that has been created for the broadest representation of Internet stakeholders to share information on topical public policy issues and promote good practice in matters relating to the access and use of the Internet.

CIGF derives from the Commonwealth's ICT4D Programme known as *Commonwealth Connects*. This Programme aims to facilitate technology and knowledge transfer between member states and institutions.

The CIGF asked people what they thought the challenges were arising from the Internet's proliferation and our increasing reliance on it in the home, our places of work, in the classroom and for the conduct of all manner of business. Coming close to the top of a long list was child protection.

We are indebted to John Carr for this compilation of legal measures, good practice and other resources on the subject which we have brought together in this toolkit. John is one of the foremost global experts in this field and we have indeed been fortunate in having his services placed at our disposal to pull together this body of work. We would also like to acknowledge the particular contributions of the International Centre for Missing and Exploited Children (ICMEC), the ITU, the Children's Charities' Coalition on Internet Safety, whose material is referenced widely in this work, and the GSM.

The primary audience for the toolkit is the Commonwealth but it is hoped that it might be of interest to a wider range of countries and professionals with an interest in child protection. This is the second version of the toolkit. It updates the first one, published in 2010. We very much hope to be able to publish further updates as circumstances change over time.

Joseph V. Tabone

Chairman

Commonwealth Internet Governance Forum

vv

introduction

Among other things this report describes the impact of the Internet on the production and distribution of child pornography, now often referred to as *child abuse images* since this more accurately describes the nature of the visual depictions in question. It makes a number of suggestions about how states can join in the global fight against this vile misuse of cyberspace.

In particular the report presents a range of legal measures which Commonwealth Member States might consider adopting and it sets them in the context of wider initiatives designed to make the Internet a safer place for children and young people the world over.

the impact of the internet on child pornography

In 2006, Special Rapporteur Paulo Sérgio Pinheiro presented the UN General Assembly with his "Report of the independent expert for the United Nations Study on violence against children."[1] In the report, Pinheiro noted[2] that

"The Internet and other developments of communications technologies...appear to be associated with an increased risk of sexual exploitation of children as well as other forms of violence (against children)."

In relation to online child pornography the evidence that this is so is now beyond any doubt.

Prior to the arrival of the Internet, in many parts of the world it was extremely difficult to obtain child pornography. A person interested in acquiring such material generally either needed to know a person who already had some or go to a great deal of trouble and perhaps risk being identified and unmasked. Even as recently as the mid-1990s one distinguished expert on child protection was able to describe the traffic in child pornography as being "a cottage industry"[3]. Today the images can be a mouse-click away and their exchange takes place on a global scale. In the early days of the Internet a substantial amount of the trade in child abuse images was commercial

1 See http://www.unicef.org/violencestudy/reports/SG_violencestudy_en.pdf.
2 At Para 77.
3 People Like Us, Sir William Utti , HMSO, London 1997.

in nature, often linked to organized crime. This still exists to some degree but now much of the interchange is "like for like" among collectors of varying degrees of technical sophistication[4].

Using 1995[5] as the baseline, INTERPOL reported knowing of only around 4,000 unique child pornographic images in total worldwide[6]. The number of individual children depicted in these images could be counted in hundreds. There is a marked growth in images of younger children being subjected to ever more violent and depraved sexual acts[7].

Data recently supplied by INTERPOL and data published in the UK[8] and Italy[9] suggest that the number of known unique images has grown to around 1 million, and the number of children being abused to make the images can be counted in the tens of thousands[10]. UNODC has suggested that perhaps as many as 50,000 new images are going into circulation each year[11], although this may now be regarded as a considerable underestimate as it was made before the growth in sexting: a process which involves minors making sexualised images of themselves and sending them to "friends" who very often later publish them on the Internet where they then find their way into paedophilic collections[12].

It is anyone's guess how often the images and their duplicates are downloaded or exchanged online and offline but, judging by the numbers seized in different police actions around the world[13], it is very likely to run into billions per annum. In pre-Internet days, typically police officers would arrest individuals who possessed only a handful of child pornography images. In unusual cases there might be hundreds of pictures. In the whole of 1995, the police in Greater Manchester in the UK seized the grand total of 12[14], all on paper, whereas a few years later the same police force, covering exactly the same geographical area and roughly the same population, arrested John Harrison of Denton, with approximately 1 million images in his possession, all stored on computers or digital media[15]. In June 2009, in a single action, police in Mexico arrested a Canadian citizen, Arthur Leland Sayler, in possession of 4 million images.

---

4 http://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf.

5 Arguably the last year before the Internet boom erupted in many countries.

6 Correspondence with John Carr. The British police reported that in 1990 they were aware of 7000 unique images in the UK,

7 See https://www.iwf.org.uk/assets/media/IWF%20Annual%20Report%202007.pdf, page 8. In addition, because of the differences in the definition of child pornography used by various countries it is likely that these numbers understate what many nations would consider to be the true volumes of known child pornographic images.

8 See http://www.official-documents.gov.uk/document/cm/77/7785/7785.pdf page 7.

9 Telefono Arcobaleno speaks of 36,000 children of whom 42% are under 7 years of age and 77% are under the age of 12. See www.telefonoarcobaleno.org/pdf/tredicmoreport_ta.pdf, page 8.

10 And bear in mind these numbers are based solely on what is known about through successful police actions. The true volume is likely to be higher.

11 http://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf.

12 http://www.iwf.org.uk/about-iwf/news/post/363-self-generated-image-study—final-paper-published.

13 http://johnc1912.wordpress.com/2012/10/16/i-thought-i-was-unshockable-2/.

14 Correspondence with John Carr.

15 See http://tinyurl.com/manchestermillion.

The trend in convictions is another signifier. Once more taking 1995 as the baseline, in the UK[16] 142 people were cautioned or proceeded against for child pornography offences. In 2007 there were 1,402[17]. Comparisons between 1995 and 2007 in terms of Internet usage are not very meaningful because broadband barely existed in 1995, while by 2007 it had become commonplace. In 1995, fewer than two million UK households had Internet access (primarily dialup), whereas by 2007 the number of households with Internet access was up to 15.23 million, of which 84% had broadband[18].

Even though there are as yet no reliable, systematic ways of making international comparisons either in terms of arrests, convictions or the volume of images being seized, it is apparent that no nation is exempt[19]. There is a strong link between Internet crimes of this kind and the growth in the number of broadband connections within a country. As the rate of take up of broadband in many Commonwealth countries starts to climb, Governments and police agencies will therefore want to put in place measures to head off or deal with this problem as part of a wider ranging series of child protection policies and programmes[20].

Elements of the Internet industry have been very keen to work with Governments and law enforcement agencies across the world to drive out child pornography from the Internet as a whole and especially from their own networks. Partly as a result there are some highly successful models in place in several Commonwealth countries which can provide extremely useful pointers. The mobile phone industry has been extremely active in this respect, having developed a widely supported global Mobile Alliance Against Child Sexual Abuse Content[21].

16 It is extremely difficult to obtain reliable standardised or comparable data from other jurisdictions.

17 Offending and Criminal Justice Group (RDS), Home Office, ref: IOS 503-03.

18 See http://www.statistics. gov.uk/pdfdir/inta0807.pdf.

19 Early police actions, e g. Operation Cheshire Cat (http://articles.chicagotribune.com/1998-12-11/news/9812110378_1_child-pornography-internet-site-wonderland-club) and Operation Cathedral (http://en.wikipedia.org/wiki/Operation_Cathedral) underlined the scale and international character of the exchange of child pornography.

20 Several Commonwealth countries - Barbados, Bangladesh, Fiji, Grenada, Lesotho, Malaysia, Mauritius, Rwanda, South Africa, Seychelles, Swaziland, Trinidad and Tobago, UK and Zambia - participated in the ITU's Child Online Protection survey, published in June 2010 (http://tinyurl.com/itusurvey) which also showed that concern about the availability of online child pornography was shared by Governments across the world.

21 See http://www.gsma.com/publicpolicy/myouth/mobiles-contribution-to-child-protection/mobile-alliance.

the harm caused by child pornography

The many different ways in which sexual abuse can damage children is well documented[22] [23]. The Internet has brought a new dimension to the harm caused by the originating illegal act. It adds to and magnifies the abusive act in the following ways:

The images undermine the child's self confidence and self-esteem

Child pornography is a visual record of abuse and humiliation. A child in a pornographic image that has been uploaded to the Internet can never know, never be certain, who might have seen or downloaded the image, or who might be about to. It severely undermines the child's self-confidence and gnaws away at their self-esteem.

Every casual glance or remark, for example from a stranger on a bus, can potentially be interpreted through the prism of the possibility, the anxious embarrassing worry, that this other person has recognised them from the image.

22 For a more extensive discussion of these issues, see: http://webarchive.nationalarchives.gov.uk/20130401151715/https://www.education.gov.uk/publications/eOrderingDownload/00305-2010DOM-EN.PDF.

23 See Safeguarding Children and Young People from Sexual Exploitation, DCSF, June 2009, page 22, t

The images are a gross violation of the child's right to privacy

In any and all proceedings concerning the abuse of a child, the courts and the professional staff working with the child normally go to extraordinary lengths to preserve the anonymity of the victim. That is rooted in sound therapeutic principles. If nothing else, the production and publication of child pornography on the Internet should be considered a gross violation of the child's right to privacy. By definition there can be no question of consent as to the production and publication of the image.

Further or repeated publication of the images re-abuses and re-victimizes the child

For as long as the images remain on public view on the Internet the child is in a very real sense being "re-abused" or is being put at risk of further harm every time the pictures or videos are viewed or downloaded. For this reason people who deliberately engage in viewing or downloading the images are in reality child abusers by proxy.

Publication risks creating new child abusers

There is a growing body of evidence which suggests that people who deliberately download and collect child pornography are significantly more likely than the general population to commit offences[24] against children, either online or in the real world, or both[25]. Not all downloaders will be equally dangerous to children, and many will not reoffend once caught, particularly if they are helped to manage their future behaviour and are supported by appropriate forms of monitoring or supervision. However, great caution is nonetheless always required because of the difficulties associated with predicting how any given individual might behave in the future.

Images can fuel downloaders' fantasies, spurring them on to commit further illegal acts. That is the second major reason for wanting such images to be removed from view as quickly as possible: to the extent that the images sustain or encourage paedophile activity, the continued availability of the images puts yet more children at risk in other

24 In addition to the offence of downloading images.

25 See for e. g. Self-Reported Contact Sexual Offenses by Participants in the Federal Bureau of Prisons' Sex Offender Treatment Program: Implications for Internet Sex Offenders, Hernandez, November 2000, presented at the Association for the Treatment of Sexual Abusers (ATSA) in San Diego, California, also From Fantasy to Reality: the Link Between Viewing Child Pornography and Molesting Children. Kim, C (2004), based on data from the US Postal Inspection Service, Kim, C, and Internet traders of child pornography and other censorship offenders in New Zealand: Updated Statistics (November 2004), Wilson and Andrews.

ways. Removing the images at the source or, better yet, preventing their initial distribution or uploading will therefore help reduce the number of potential new online and offline child abusers.

Criminal networks

The criminal networks behind many of the commercial child abuse web sites are often not populated by paedophiles in the ordinary sense. These perpetrators systematically arrange for children to be raped by others solely in order to photograph and film the rape as a prelude to selling the pictures for profit.

If it is seen that the circulation of illegal images can survive and prosper on the Internet, there is a risk that it will encourage others to come into the market and thereby add to the spiral of child sexual abuse, but more widely it may also encourage individuals active in other types of crime to believe that the Internet is a safe place for them to go to carry on their activities. Attacking the presence of child pornography on the Internet is therefore not only important in its own right; it is also a key part of building trust and confidence in the Internet as a medium for e-commerce and for other interactions

The drift towards less regulated environments

As with money laundering and a number of other criminal activities, there are already some preliminary indications that persons wishing to promote or supply child pornography on the Internet will look for jurisdictions where the legal framework is weak or where the capacity of local law enforcement is limited or constrained. This allows the criminals to act with minimal or no interference. Thus, as a number of countries begin to improve their legal framework and attendant capability to fight these types of crimes there is a risk that countries, which are slower to act or less well prepared, will become a magnet for housing or publishing child pornography.

a framework of laws

Several widely adopted international treaties and conventions contain provisions which require signatories to prevent the distribution of child pornography within their jurisdiction and to protect children from becoming victimized by it. Foremost among these is the UN Convention on the Rights of the Child[26]. Also of note are the Council of Europe Convention on Cybercrime[27] and the Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (the Lanzarote Convention)[28].

In December, 2011, the European Union adopted an EU-wide law on combating the sexual abuse and sexual exploitation of children and child pornography[29]. It requires every Member State to ensure that they have the necessary machinery in place to facilitate the removal of any child pornography that might be found on web sites housed within their jurisdiction. The same Directive also authorizes Member States to block access to web sites containing child pornography where the web site is being hosted outside of their own jurisdiction.

For a course of action against child pornography on the Internet to be sustained over time, and for it to be capable of being integrated into multinational law enforcement

26 Convention on the Rights of the Child, G. A, Res. 44/25, 61st plen. mtg., U.N. Doc. A / RES/ 44/25 (Nov. 20, 1989), entered into force Sept. 2, 1992; see also Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, G. A . Res. 54/263, Annex II, U.N. Doc. A/54/49, Vol. III, art. 2, para. c, entered into force Jan. 18, 2002, see http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx.

27 Council of Europe Convention on Cybercrime, Nov. 23, 2001, see http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

28 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Oct. 25, 2007, at http:/conventions.coe.int/Treaty/EN/treaties/Html/201.htm. The final communique of the 3rd World Congress Against the Sexual Exploitation of Children and Adolescents, held in Brazil in November 2008, contains a summary of measures being taken in this area, see http://www.chis.org.uk/uploads/07a.pdf.

29 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:EN:PDF.

activities, it must be firmly rooted in domestic law.

The U.S.-based International Centre for Missing & Exploited Children (ICMEC)[30] conducts a regular survey entitled "Child Pornography: Model Legislation & Global Review" (Model Legislation Report). The survey examines the legal framework of countries around the world to determine whether national legislation:

1. Exists with specific regard to child pornography;

2. Defines child pornography;

3. Criminalizes computer-facilitated offences involving child pornography;

4. Criminalizes the knowing possession of child pornography regardless of the intent to distribute; and

5. Requires Internet Service Providers to report suspected child pornography to law enforcement or another designated agency.

In the 1st edition of the survey, published in 2006[31], of the then 184 member countries of INTERPOL, only 27 had what ICMEC considered to be "legislation sufficient to combat child pornography offences". This meant that only 27 countries satisfied at least four of the criteria outlined above[32].

95 countries had no legislation that specifically addressed child pornography. Of the remainder that did have legislation that referred to child pornography, 41 nonetheless did not criminalize the knowing possession regardless of the intent to distribute and 27 did not have legislative provisions to criminalize computer-facilitated offences in relation to child pornography.

The 6th edition of the Review, released in August 2010, included 196 countries and showed some progress since the initial report in 2006. 44 countries met conditions one to four, however 89 countries still had no legislation that specifically addressed child pornography. Of the remaining countries that did have legislation specifically addressing child pornography 53 countries did not define child pornography in law, 33 countries did not criminalize the knowing possession regardless of intent to distribute, and 18 made no provision for computer-facilitated offences in relation to child pornography.

30 See http://www.icmec.org.

31 The 1st edition of the Model Legislation Report is on file with ICMEC.

32 Only 5 states met all five criteria. Criteria 5, mandatory reporting by ISPs, was a key area of difference, but it is acknowledged that countries have varying approaches or traditions in relation to reporting of crimes.

ICMEC published the 7th edition of the review in March 2013[33]. It shows marked improvements worldwide. The new results indicate that 69 countries now meet at least 4 of the criteria, while approximately 53 still have no legislation in regards to child pornography. There has been legislative movement in 100 countries since 2006.

Since this Toolkit was first released in 2010, there has been substantial improvement in the number of Commonwealth countries that have introduced or improved legislation regarding child pornography. In 2010, a significant number of Commonwealth countries met none of the five criteria, whereas others met fewer than the minimum four considered necessary to deal with this type of crime. At that time, of the 53 Commonwealth Member States, only 11 countries had legislation deemed to be sufficient to combat child pornography. The number of countries with legislation deemed to be sufficient has now doubled with 22 countries meeting at least four of the criteria.

33 http://www.icmec.org/en_X1/pdf/Child_Pornography_Model_Law_English_7th_Edition_2012.pdf.

a commonwealth initiative

The Commonwealth wishes to promote an initiative to ensure that all Member States meet criteria one to four of the ICMEC Model Legislation Report. Doubtless some will want to adopt all five criteria, depending on their traditions in relation to the mandatory reporting of crime more generally.

In developing a programme of this kind the local Internet and mobile phone industries are very likely to want to be key partners and allies in elaborating the potential approaches at a technical, operational and policy level.

Borrowing heavily from the EU Directive referred to earlier[34], in Appendix IV, a skeleton outline is provided which would give effect to all of the substantive legal elements outlined in ICMEC's Model Legislation Report.

Because the EU Directive does not make ISP reporting mandatory, the model wording for mandatory reporting provided in Appendix IV is adapted from Canadian law[35].

In common with the EU Directive and existing practice in several Commonwealth countries, Appendix IV includes a reference to outlawing so-called pseudo images.

With the advent of powerful video and photographic editing software it is possible to create life-like images of events which, in reality, did not actually take place. Where it can be established that such software has been used, in some jurisdictions, e.g.

34 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:EN:PDF.

35 Ontario Child Pornography Report Act, 2008, see http://tinyurl.com/ontariolaw.

the USA, the images may not be classified as child pornography[36]whereas in others, e.g. the UK, the use of editing software is irrelevant. If something looks like child pornography it is treated as if it is in fact child pornography. However, in the UK, if the defence can show that the image is pseudo, upon conviction it can lead to a reduction in the sentence given[37].

The UK courts also adopted a system for classifying images according to the severity of the abuse depicted. This impacts on the sentences handed out by the courts following conviction[38].

The system was based on work originally carried out by the COPINE Project in the University of Cork[39].

36 Although it could still be obscene. http://www.law.cornell.edu/supct/html/00-795.ZS.html; Ashcroft v Free Speech Coalition, 535 U.S. 234 (2002).

37 See R v Oliver and others (2003) 2 Cr. App.R .28 for the sentencing guidelines including the original classification system. Also see http://www.cps.gov.uk/publications/code_for_crown_prosecutors/mode.html, where inter alia, the amended classification system is set out in the section headed "Mode of Trial".

38 Ibid.

39 Ibid.

related measures

Outlawing child pornography in the manner anticipated by the ICMEC framework and as set out above is a necessary step in any comprehensive plan to make the Internet safer for children. However, other measures are needed to develop a holistic approach to online child protection:

Solicitation of children for sexual purposes

Paedophiles can use the interactive components of the Internet to strike up highly manipulative relationships with children online. In some countries this is referred to as "grooming". ICMEC will in the future be monitoring anti-grooming legislation on a regular basis. Early indications suggest that many Commonwealth countries are already taking action[40].

These manipulative relationships can result in a child creating and transmitting sexualized images or sexualized videos of themselves. This is sometimes referred to as "sexting"[41]. These images and videos can be captured and reproduced as child pornography, or a child could be persuaded or blackmailed into meeting the paedophile offline for illegal sexual activity. Both may occur. While in some cases the full extent of the exploitation takes place online[42].

---

40 Australia, Botswana, Brunei Darussalam, Cameroon, Canada, Guyana, India, Jamaica, Malta, New Zealand, Singapore, South Africa, Trinidad & Tobago, and U.K.

41 See also earlier reference on page 7.

42 "Alarming New Trend in Online Sexual Abuse." Published by the Child Exploitation and Online Protection Centre. Available at https://www.ceop.police.uk/Media-Centre/Press-releases/2013/ALARMING-NEW-TREND-IN-ONLINE-SEXUAL-ABUSE/.

Thankfully, these types of cases are comparatively unusual, but the consequences for the child can be catastrophic which is why it is important to ensure that the legal framework needed is up to date and fit for purpose.

Having a provision which expressly outlaws grooming behaviour typically will make it possible for law enforcement to intervene at an earlier stage in the cycle of abuse without having to wait for the substantive act to be attempted or completed. Many countries have adopted such a law. A skeleton outline is provided in Appendix V, extracted from the EU Directive on combating the sexual abuse and sexual exploitation of children and child pornography [43].

The need for a hotline: getting images removed from the Internet

Reports from members of the public have been key to identifying the location of child pornography on the Internet. The reports are made to a "hotline", which typically will work closely with the police and the Internet industry. Some of these reports have led to substantial police actions, occasionally on a global scale.

Practice varies between hotlines. Some act largely as "post boxes", simply passing on information received from the public without checking or verifying it. In other hotlines staff will look at the report and confirm whether or not the reported image is illegal[44]. If it is illegal and it is housed within their own jurisdiction, a notice can be issued to the hosting company requiring them to remove it while simultaneously allowing the police to initiate an investigation. In most jurisdictions as long as the hosting company acts swiftly to take down the image they will not be liable for having hosted it unknowingly.

In situations where the image is housed overseas an international network of hotlines exists which can facilitate an exchange of information. This international network, INHOPE[45], also has a key role in setting the professional standards by which all hotlines should operate.

It may not strictly-speaking be necessary for every individual country to operate its own hotline. Groups of smaller countries could combine to establish a shared service or they could work with an existing hotline. Some of the larger existing hotlines may be able

43 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:EN:PDF.

44 This means the hotline staff will take a view on whether the reported image is likely to be judged to be illegal in their country. The processes governing such decisions should be clearly stated, be governed by the principles of natural justice and be subject to appeal.

45 http://www.inhope.org/gns/home.aspx.

to allow agencies in other countries to use their "back end" as a means of reducing operational costs[46]. A paramount consideration is the mother-tongue of the countries concerned; however, it is also essential to win the buy-in of the relevant parts of the local law enforcement community.

Police forces from Australia, Canada, Europol, Indonesia, INTERPOL, Italy, Korea, the Netherlands, New Zealand, the United Arab Emirates, the UK and the USA have developed the Virtual Global Taskforce[47], a form of hotline to facilitate the reporting of suspected crimes against children taking place in real time e.g. in chat rooms or other interactive forums.

Blocking

Where illegal images are detected on servers which lie outside the jurisdiction of a given country it has been known for it to take a month or more, sometimes substantially more, for the material which has been identified to be removed from the remote server. To deal with this problem a practice referred to earlier and known as "blocking" has emerged in a number of Commonwealth and other countries. Blocking measures are most commonly deployed by access providers, typically Internet Service Providers, but the world's large search engines also deploy tools specifically aimed at denying access through them to known web addresses containing child pornographic images[48].

To facilitate blocking a list of the URLs of sites or web pages containing illegal images can be obtained from one or more of the existing hotlines around the world. In addition, through its established machinery INTERPOL can also supply a list of sites which pass their minimum threshold[49].

Law enforcement and other workforce requirements

In order to implement the laws on online child pornography effectively, and in order to be able to participate in international police actions in this field, each country will require appropriately trained law enforcement officials and a range of forensic facilities. The cost of training and the cost of the necessary equipment have declined in recent years and there are a number of potential sources of support and assistance. In the first instance, INTERPOL may be a useful point of reference. ICMEC continuously provides law

46 The UK's hotline, the Internet Watch Foundation, is an example.

47 http://www.virtualglobaltaskforce.com/.

48 For a fuller discussion of this issue see: http://www.chis.org.uk/2010/07/25/briefing-on-child-abuse-images-and-blocking.

49 INTERPOL refer to this list as being "the worst of the worst." It contains images that are very likely to be illegal in ever y jurisdiction in the world. e. g. because they contain examples of abuse of prepubescent children.

enforcement and prosecutor training in all parts of the world.

Social workers, teachers and others who are involved with children in a professional capacity will also need training to recognise and understand online victimization, the signs of victimization and its potential consequences for the child affected as well as his or her family.

Identifying child victims and the interests of the child

A comparatively small number of children depicted in child pornographic images are ever located in real life. In collaboration with law enforcement, the U.S.-based National Center for Missing and Exploited Children had, at the time of writing, identified just over 5,200 different children from images in their database[50]. Other agencies outside of the USA account for a similar number[51]. The challenges can be substantial, especially if there are no clues in the image to indicate the country where the child lives or where the offence took place.

A number of databases of images are being developed by INTERPOL and other police agencies. Amongst other things[52] these will help speed up investigations. These databases should make it straightforward and quick for a law enforcement officer in a given country to determine whether a particular image is already known and, if so, what the outcome was of any investigation that might have taken place.

Where a child is identified and located in real life, great care will need to be taken in planning any rescue of the child or other form of intervention. A partnership approach between law enforcement and other agencies, such as child advocacy centres, is likely to be critical to ensuring that the needs of the child are met. Law enforcement needs to value the role and importance of child protection. The best interests of the child must be the key determinant of any and all courses of action.

Peer2Peer networks, the Darknet and hashes

Since the publication of the first edition of this toolkit it has become clearer to law enforcement agencies that while the worldwide web remains a major source of child abuse images, larger and larger volumes are now being exchanged between collectors

50 Based on correspondence between the authors. However this number also includes child victims reported to NCMEC where it was not necessarily confirmed that the sexually abusive images were published widely on the Internet.

51 Based on correspondence with John Carr.

52 See next section for how image hashes can also be used in another way.

who are using Peer2Peer networks[53], "onion servers"[54], encryption[55] and other highly sophisticated technical methods to disguise their activities online. The emergence of cloud computing with substantial volumes of inexpensive or free online storage facilities has also opened up access to filesharing sites on a substantial scale.

In Peer2Peer and filesharing environments there may be scope for tracking down already known illegal images through using their hash values[56]. Microsoft developed a programme called PhotoDNA[57] which is available at no cost to help with the deployment of hashes. Other programmes may be able to perform similar functions either to detect illegal images already being stored or to prevent them being uploaded.

Liaison with the financial services industry

The major credit card companies and banks in the USA and Europe have been collaborating with law enforcement to close down their systems to persons seeking to exchange child abuse images on a commercial basis. However, other means of making anonymous or difficult to trace payments online are still available.

A confidential manual on how to detect and prevent online payments systems from being abused for the purposes of selling or exchanging child pornography was prepared in May 2007, by the US-based Financial Coalition Against Child Pornography[58]. A similar document was produced by the European Financial Coalition in 2010[59]. ICMEC is engaged in the Asia-Pacific region to produce comparable guidelines[60] [61].

Action in relation to abuses of the domain name system

A substantial proportion of the information provided to individual domain name registrars, and published in the WHOIS directory, concerning the persons or legal entities who own or manage particular domains is either false, incomplete or unverifiable[62]. Moreover the domains with false, incomplete or unverifiable ownership information are where a high proportion of criminal conduct online originates.

53 http://en.wikipedia.org/wiki/Peer-to-peer.
54 https://en.wikipedia.org/wiki/Tor_(anonymity_network).
55 http://en.wikipedia.org/wiki/Encryption.
56 http://en.wikipedia.org/wiki/Hash_function.
57 http://www.microsoft.com/en-us/news/presskits/photodna/.
58 http://www.icmec.org/en_X1/pdf/FCACPBackgrounder1-13.pdf.
59 http://www.europeanfinancialcoalition.eu/private10/images/document/8.pdf.
60 http://www.icmec.org/missingkids/servlet/PageServlet?LanguageCountry=en_X1&PageId=4355.
61 http://www.icmec.org/en_X1/pdf/FCACP_APAC-_AOReport__January_2013_.pdf.
62 http://johnc1912.wordpress.com/2012/02/06/who-is-reading-the-whois-review-part-1/.

It should not be so easy for the domain name system to be misused in this way, whether in relation to persons publishing or promoting access to child pornography or persons engaging in other types of crimes. The Internet Corporation or Assigned Names and Numbers (ICANN)[63] is the world body responsible for administering the domain name system. At ICANN's meeting in Brussels in June 2010 this matter was discussed by the Governmental Advisory Committee (GAC)[64]. The GAC encouraged ICANN and Registrars to work with law enforcement agencies to address concerns arising from the misuse of the domain name system[65]. During discussion at the same GAC meeting some GAC members proposed requiring relevant Registrars to strengthen their procedures for ensuring that the information provided when registering or buying a new domain name or in relation to sustaining an existing domain name is verifiably accurate[66].

Every Commonwealth Government can discuss these issues directly with the agencies which administer their country level domains. The Commonwealth Security Organization, the Commonwealth-IGF Secretariat, and the Commonwealth Cybercrime Initiative would be happy to advise further in respect of these matters.

Other legal provisions

It is beyond the scope of a report of this kind to make any detailed recommendations in relation to sentencing, the forfeiture of assets, the capacity of corporate entities to commit crimes, aggravating or mitigating circumstances, the provision of sex offender treatment programmes, supervision orders or sex offender registers and similar issues, but it is likely that consideration will need to be given to matters of this kind in the interests of establishing a complete and rounded policy framework.

Education and awareness measures and broader approaches

Up to this point the report has looked at the issue of child pornography in a tightly focused way. Many Commonwealth Member States will doubtless also want to promote, or continue to promote, a much more extensive set of policies which address many more aspects of online child safety.

For example, a key challenge is to ensure that children and young people themselves are

63 See http://www.icann.org/.
64 Every Commonwealth Government is eligible to join the GAC and attend its meetings.
65 See http://domainincite.com/docs/GAC-post-Brussels-communique.pdf
66 See http://brussels38.icann.org/node/12448.

aware of a range of hazards which exist on the Internet e.g. exposure to age inappropriate but legal content, exposure to unscrupulous commercial practices, the risk of Internet addiction and, hugely important for young people of school age and others, the risks associated with various forms of online bullying.

Children and young people need to be taught how to avoid these things altogether and to learn strategies for dealing with them should they nonetheless occur. They need to develop resilience and know how to extricate themselves swiftly and safely from difficult situations. Just as children and young people need to be taught these things, so too do their parents and teachers in order that they can both provide help and support, but also so they can assume their proper role and responsibilities for the children in their care.

Technical measures such as filtering software can play some part in supporting good practices online, but technical measures alone will never be enough. The best defence for a child is their own knowledge and resourcefulness backed by the support and attention of a responsible adult. Schools and community-based organizations can play a key role in developing awareness raising initiatives around online safety.

There is a great wealth of educational and awareness materials available on the Internet and sometimes also in printed form for children and young people, for their parents, for schools and for law enforcement. Individual companies, trade associations, Governments and police agencies around the world have produced what sometimes seems like an almost overwhelming amount, in a variety of languages. Much has been developed within a framework of self regulatory models that several Governments have sponsored as a means of dealing with the new challenges that the Internet poses.

The quality of educational and awareness material available can vary enormously, from the mediocre to the truly superb. In the latter category, and perhaps the closest there is to a global single point of contact in this field, is the set of documents and associated assets and links produced by the International Telecommunication Union (ITU) under its Child Online Protection (COP) initiative[67]. The European Union's Safer Internet Programme[68], particularly the INSAFE initiative[69] and the TeachToday website[70], are also tremendously valuable resources producing high quality materials.

The ITU's COP continues to be a major strand of activity within the framework of the ITU's overall work on online security, the implementation of the Global Cybersecurity Agenda and the implementation of Action Line C5 of the World Summit on the Information

67 See http://tinyurl.com/copinit (the authors of this paper were very closely involved in the preparation of the COP documents).
68 See http://tinyurl.com/sipprog.
69 See http://tinyurl.com/insafehome.
70 See http://www.teachtoday.eu/.

Society[71]. In that capacity the ITU may also be an important source of help and advice in progressing policy in this area in Commonwealth Member States.

71 See http://www.itu.int/osg/csd/cybersecurity/WSIS/index.phtml.

appendix I

Commonwealth Member States that do not meet any of the 5 ICMEC criteria

1. Antigua & Barbuda
2. Dominica
3. Ghana
4. Grenada
5. Guyana
6. Kiribati
7. Lesotho
8. Maldives
9. Mozambique
10. Namibia
11. Nauru
12. Pakistan
13. St. Lucia
14. Samoa
15. Solomon Islands
16. Swaziland
17. Tuvalu

appendix II

Commonwealth Member States that meet between 1 and 3 of the ICMEC criteria

1. Bangladesh
2. Belize
3. Fiji
4 Gambia, The
5. Malaysia
6. Nigeria
7. United Republic of Tanzania
8. Zambia
9. Kenya
10. Rwanda
11. Singapore
12. Mauritius
13. St. Kitts and Nevis
14. Seychelles
15. Sri Lanka

appendix III

Commonwealth Member States that meet between 4 and 5 of the ICMEC criteria

1. Bahamas
2. Barbados
3. Botswana
4. Brunei Darussalam
5. Cameroon
6. Cyprus
7. Jamaica
8. Malawi
9. Malta
10. New Zealand
11. Papua New Guinea
12. St. Vincent and the Grenadines
13. Sierra Leone
14. Tonga
15. Trinidad and Tobago
16. Uganda
17. United Kingdom
18. Vanuatu
19. Australia
20. Canada
21. India
22. South Africa

appendix IV

Draft legislative proposals

1. Definition of child pornography

a. 'child' shall mean any person below the age of 18 years;
b. 'child pornography' shall mean
    i. any material that visually depicts a child engaged in real or simulated sexually explicit conduct; or
    ii. any depiction of the sexual organs of a child for primarily sexual purposes; or
    iii. any material that visually depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of any person appearing to be a child, for primarily sexual purposes; or
    iv. realistic images of a child engaged in sexually explicit conduct or realistic images of the sexual organs of a child, regardless of the actual existence of such child, for primarily sexual purposes.

2. Offences concerning child pornography

a. It shall be a punishable offence to:
    i. Knowingly obtain access to, publish, download or distribute child pornography by means of information and communication technology or any electronic network;
    ii. Acquire or possess child pornography;
    iii. Disseminate, advertise, promote access to or transmit child pornography;
    iv. Supply or otherwise make available child pornography;
    v. Produce child pornography;
    vi. Cause a child to participate in child pornographic performances;
    vii. Profit from or otherwise exploit a child participating in child pornography;
    viii. Recruit a child to participate in child pornographic performances.

3. Mandatory Reporting

a. Any person who has reasonable grounds to believe that a representation or material found on any electronic network or electronic device or storage medium is child pornography shall immediately report the matter to a reporting entity;
b. Reporting entities and the duties of reporting entities shall be designated by regulation;
c. Subsection (a) applies notwithstanding that the information on which the belief is founded is confidential and its disclosure is otherwise prohibited by law;
d. Nothing in this Act authorizes or requires any person to seek out child pornography;
e. No action lies against a person for reporting information pursuant to subsection a unless the reporting is done falsely and maliciously;
f. It shall be a punishable offence knowingly to make false and malicious reports;
g. Failure to comply with subsection (a) is a punishable offence save where the information in question is governed by attorney-client privilege.

appendix V

Solicitation of children for sexual purposes

It shall be a punishable offence for any adult, by means of information and communication technology or any electronic network, to arrange to meet a child who has not reached the age of sexual consent under national law, for the purpose of committing a sexual offence, where the proposal to meet is followed by any material act on the part of the adult which is intended to facilitate or bring about the meeting with the child.

2012

Online Child Protection

Commonwealth IGF