2010

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.

The initiative to set up CIGF derives from the Commonwealth's ICT4D Programme known as Commonwealth Connects. The purpose of this Programme is to facilitate technology and knowledge transfer between member states and institutions.

In setting up the IGF we asked people what they saw as the issues relating to the Internet's proliferation and our increasing reliance on it in the home, our place of work, in the classroom and for the conduct of all manner of business. Coming close to the top of a long list of these was the issue of child protection and the Internet. We are indebted to John Carr for this compilation of legal measures, good practice and other resources on the subject . 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 contribution of the International Center for Missing and Exploited Children (ICMEC), ITU and the Children's Charities Coalition on Internet Safety whose material is referenced widely in this work and the GSM organisation who plans to participate in its dissemination.

This compilation is the first version collated for our Commonwealth audience. This will be periodically updated as more relevant information becomes available.

Joseph V. Tabone
Chairman
Commonwealth Internet Governance Forum

introduction

This report describes the impact of the Internet on the production and distribution of child pornography. It presents a range of legal measures which Commonwealth Member States might consider adopting and 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, United Nations Special Rapporteur Paulo Sérgio Pinheiro presented to the UN General Assembly his "Report of the independent expert for the United Nations study on violence against children[1]." In the report, Pinheiro noted[2] that

"The [I]nternet 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 overwhelming.

Prior to the arrival of the Internet, in many parts of the world it was

1 See http://tinyurl.com/3a52zpt.
2 At Para 77.

extremely difficult to obtain child pornography. A person interested in acquiring child pornography, generally either had to know someone who had such images or go to great trouble and take personal risks to obtain the images on their own. Even as recently as the mid-1990s, one distinguished expert on child protection was able to describe the

exchange of child pornography as being "a cottage industry[3]" . Now the images are a mouse-click away. It is a global industry that may be worth millions of dollars to those who engage in it for financial gain[4].

Using 1995 as the baseline[5], Interpol reported knowing of 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. Data recently supplied by Interpol and data published in the UK[7] and Italy[8] suggest that today the number of known unique images is around 1 million, and the number of children being abused to make the images is in the tens of thousands[9]. There is a marked growth in images of younger children being subjected to ever more violent and depraved sexual acts[10].

It is anyone's guess how often the images and their duplicates are

3 People Like Us, Sir William Utting, HMSO, London 1997.
4 See http://www.justice.gov/opa/pr/2001/August/385ag.htm.
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, see http://www.official-documents.gov.uk/document/cm77/7785.pdf.
7 See http://www.official-documents.gov.uk/document/cm/77/7785/7785.pdf, page 7.
8 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.
9 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.
10 See http://preview.tinyurl.com/iwfreppage8, 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.

downloaded or exchanged online and offline but, judging by the numbers seized in different police actions around the world, 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 images. In the whole of 1995, the police in Greater Manchester in the UK seized the grand total of 12 images, all on paper[11], 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[12]. In June 2009, in a single action, police in Mexico arrested a Canadian citizen, Arthur Leland Sayler, in possession of 4 million images.

The trend in convictions is another signifier. Once more taking 1995 as the point of comparison, in the UK[13] 142 people were cautioned or proceeded against for child pornography offences. In 2007 there were 1,402[14]. 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[15]. In 1995, fewer than two million UK households had Internet access (primarily dial-up), whereas by 2007 the number of households with Internet access was up to 15.23 million, of which 84% had broadband[16].

Even though there are as yet no reliable, systematic ways of making

11 Correspondence with John Carr.
12 See http://tinyurl.com/manchestermillion.
13 It is extremely difficult to obtain reliable standardised or comparable data from other jurisdictions.
14 Offending and Criminal Justice Group (RDS), Home Office, Ref: IOS 503-03.
15 Broadband access is important because it makes accessing large files easier and more practical. Typically child pornography and videos will be large files.
16 See http://www.statistics.gov.uk/pdfdir/inta0807.pdf.

international comparisons either in terms of arrests, convictions or volume of images being seized, it is apparent that no nation is exempt[17]. 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 want to put in place measures to proactively head off or deal with this problem as part of a wider ranging series of child protection policies and programmes[18].

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 from their own networks in particular. Partly as a result there are some highly successful models in place in several Commonwealth countries which can provide very useful pointers. The mobile phone industry has been particularly active in this respect, having developed a widely supported global Mobile Alliance Against Child Sexual Abuse Content[19].

17 Early police actions, e.g. Operation Cheshire Cat (http://tinyurl.com/cheshcat) and Operation Cathedral (http://tinyurl.com/metwond) underlined the scale and international character of the exchange of child pornography.

18 Several Commonwealth countries - Barbados, Bangladesh, Fiji, Grenada, Lesotho, Malaysia, Mauritius, Rwanda, South Africa, Seychelles, Swaziland, Trindad 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.

19 See http://tinyurl.com/moballiance.

the harm caused by child pornography

The many different ways in which sexual abuse can damage children is well documented[20][21]. 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 child pornographic image that has been uploaded to the Internet can never know, never be certain, who might have seen

20 For a more extensive discussion of these issues, see: http://publications.education.gov.uk/eOrderingDownload/00305-2010DOM-EN.PDF

21 See Safeguarding Children and Young People from Sexual Exploitation, DCSF, June 2009, page 22, http://tinyurl.com/ecmsexp.

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.

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/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 being put at risk of further harm every time the pictures or videos are viewed or downloaded. It is also why people who deliberately engage in viewing or downloading these 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[22] against children, either online or in the real world, or both[23] . 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 ways. Removing the images or, better yet, preventing their initial distribution/uploading will 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 paedophiles in the ordinary sense. They

22 In addition to the offence of downloading images.

23 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, Hernan dez, 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 Inspec tion Service, Kim, C, and Internet traders of child pornography and other censorship offenders in New Zealand: Updated Statistics (November 2004), Wilson and Andrews.

systematically arrange for children to be raped solely in order to photograph and film the rape as a prelude to selling the pictures for profit. If it is seen that this type of illegal activity can survive and prosper on the Internet, it will encourage others to come into the market and thereby add to the spiral of child sexual abuse, but it may also encourage criminals to believe that the Internet is a safe place to engage in other kinds of crimes. 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 types of 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 will become a magnet for housing or publishing child pornography.

a framework of laws

A requirement on the part of countries to prevent the distribution of child pornography within their jurisdiction and to protect children from becoming victimized by it is embedded in several widely adopted international treaties and conventions, principally the UN Convention on the Rights of the Child[24] . Also of note are the Council of Europe Convention on Cybercrime[25] and the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (the Lanzarote Convention)[26].

For a course of action against child pornography on the Internet to be

24 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 Conventioin 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://www2.ohchr.org/english/law/crc-sale.htm.

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

26 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.

sustained over time, and for it to be capable of being integrated into multinational law enforcement activities, it must be firmly rooted in domestic law.

The U.S.-based International Centre for Missing & Exploited Children[27] (ICMEC) 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[28], 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[29].

95 countries had no legislation that specifically addressed child pornography. Of the remainder that did have legislation that referred

27 See http://www.icmec.org.
28 The 1st edition of the Model Legislation Report is on file with ICMEC.
29 Only 5 states met all five criteria. Criteria 5, mandatory reporting by ISPs, was a key area of difference, but it is acknowledged that different countries have varying approaches or traditions in relation to reporting of crimes.

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[30], released in August 2010, includes 196 countries and shows some progress[31]. Now 44 countries meet conditions one – to four[32], however 89 countries still have no legislation that specifically addresses child pornography. Of the remaining countries that do have legislation specifically addressing child pornography 53 countries do not define child pornography in law, 33 countries do not criminalize the knowing possession regardless of intent to distribute, and 18 make no provision for computer-facilitated offences in relation to child pornography.

A significant number of Commonwealth countries meet none of the five criteria[33] whereas others meet fewer than the minimum four considered necessary to deal with this type of crime[34]. Of the 53 Commonwealth Member States, only 11 countries have legislation deemed to be sufficient to combat child pornography[35].

30 See http://icmec.org/en_X1/icmec_publications/English__6th_Edition_FINAL.pdf.
31 Note the baseline is larger because the 6th edition includes more than just Interpol member countries.
32 8 countries currently meet all five criteria.
33 For list of Commonwealth Member States which meet none of the 5 criteria, see Appendix I
34 For a list of Commonwealth Member States which meet between 1 and 3 of the criteria see Appendix II.
35 For a list of Commonwealth Member States which meet between 4 and 5 of the criteria, see Appendix III.

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 attitude or 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.

In Appendix IV, a skeleton outline of clauses is provided which would give effect to all of the substantive elements outlined in

ICMEC's Model Legislation Report. These borrow heavily from a draft legislative measure (Directive) published by the European Commission[36] which reflects current practice in many EU Member States. If adopted broadly in its present form, the draft EU Directive will establish a minimum uniform law for all 27 EU Member States.

The draft EU Directive does not make ISP reporting mandatory. Article 15 states:

"Member States shall take the necessary measures to encourage any person who knows about or suspects, in good faith, (that a child pornography offence has been committed) to report these facts to the competent services……"

The model wording for mandatory reporting provided in Appendix IV is adapted from Canadian law[37].

Appendix IV also goes further than the ICMEC framework in one important respect. In common with the draft EU Directive and existing practice in several Commonwealth countries, Appendix IV includes a reference to pseudo images.

With the advent of powerful video and photographic editing software it is possible to create life-like images of events that, in reality, did not actually take place. Where it can be established that such software has been used, in some jurisdictions, e.g. the USA, such images may not be classified as child pornography[38] whereas in others, e.g.

36 Draft Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, see http://tinyurl.com/draftdir.

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

38 Although it could still be an obscene image. Refer to the court decision Ashcroft v Free Speech Coalition, see http://www.law.cornell.edu/supct/html/00-795.ZS.html; Ashcroft v Free Speech Coalition, 535 U.S. 234 (2002).

the UK, the use of editing software is irrelevant. If it 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[39].

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[40].

The system was based on work originally carried out by the COPINE Project in the University of Cork[41].

39 See R v Oliver and others (2003) 2 Cr.App.R.28 for the sentencing guidelines including the original classification system used for images. Aslo see http://tinyurl.com/cpsguide, where interalia, the amended classification system is set out in the section headed "Mode of Trial".

40 See R v Oliver and others (2003) 2 Cr.App.R.28 for the sentencing guidelines including the original classification system used for images. Aslo see http://tinyurl.com/cpsguide, where interalia, the amended classification system is set out in the section headed "Mode of Trial".

41 Ibid and see http://www.ucc.ie/en/equayle/.

related measures

Outlawing child pornography in the manner anticipated by the ICMEC framework is a necessary first step; however other measures are needed to develop a comprehensive 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”. These relationships can result in the child creating and transmitting sexualized images or sexualized videos of themselves which can be captured and

reproduced as child pornography, or a child could be persuaded to meet the paedophile offline for illegal sexual activity. Very often both may occur. 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 to deal with them 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 current draft EU Directive referred to above.

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. They are made to a "hotline", which will work closely with the police. Some of these reports have led on to substantial police actions, occasionally on a global scale.

Practice varies between hotlines but in some the hotline's staff will confirm whether or not the reported image is illegal[42]. If it is illegal and it is housed within their jurisdiction, a notice can be issued to the hosting company requiring them to remove it and simultaneously allowing the police to initiate an investigation. In most jurisdictions as

42 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 clearly stated, be governed by the principles of natural justice and be subject to appeal.

long as the hosting company acts swiftly to take down the image they will not be liable for unknowingly having hosted it.

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[43], also has a key role in setting the 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 work with an existing hotline. 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 law enforcement community.

Police forces from the UK, Canada, Australia, Italy, New Zealand, Brazil, and the United Arab Emirates, together with Interpol, have also developed 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[44].

Blocking

Where illegal images are detected on servers which lie outside the jurisdiction of a given country it may take a month or more, sometimes substantially more, for the material which has been identified to be removed from the remote server.

43 See http://www.inhope.org.
44 See http://www.virtualglobaltaskforce.com.

To deal with this problem a practice known as “blocking” has emerged in a number of Commonwealth and other countries[45]. 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[46].

A list of sites containing illegal images can be obtained from one or more of the existing hotlines around the world. In addition, Interpol can also supply a list of sites which pass their threshold[47].

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 oftraining and necessary equipment has 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 and ICMEC continuously provides law enforcement and prosecutor training around the world.

Social workers, teachers and others who are involved with children

45 Australia, Canada, Denmark, Finland, Iceland, Italy, Malta, New Zealand, Norway, South Korea, Sweden, UK and USA.

46 For a fuller discussion of this issue see: http://www.chis.org.uk/2010/07/25/briefing-on-child-abuse-images-and-blocking.A provision to make blocking mandatory in every EU Member State is contained in Article 21 of the draft EU Directive referred to above.

47 Interpol refer to this list as being “the worst of the worst.” It contains images that are very likely to be illegal in every jurisdiction in the world. e.g. because they contain examples of abuse of prepubescent 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.

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. The U.S.-based National Center for Missing and Exploited Children had, at the time of writing, identified just over 3,050 different children from images in their database[48] and other agencies outside of the USA can account for a similar number[49]. 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 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

48 Based on correspondence between the authors. However this number includes images of abused children that were reported to NCMEC but which were not necessarily published on the internet.

49 Based on correspondence with John Carr.

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.

Liaison with the financial services industry

A significant part of the trade in child pornography is commercial in nature. The major credit card companies and banks in the USA and Europe have been collaborating with law enforcement to close down their systems to this type of crime. But 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 published in May, 2007, by the US-based Financial Coalition Against Child Pornography. A similar document will shortly be available from the European Financial Coalition[50].

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 which own or manage particular domains is either false, incomplete or unverifiable[51]. Moreover the domains with false, incomplete or unverifiable ownership information are where a high proportion of criminal conduct online originates. One agency found that

> "74% of child (pornography) domains…are commercial operations…

50 See http://www.ceop.police.uk/efc and http://tinyurl.com/fcapsite.
51 See http://bit.ly/ar6DMj

and 75% of these (some 850 unique domains) are registered with just 10 domain name registries."[52]

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 for Assigned Names and Numbers (ICANN)[53] 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)[54]. The GAC made encouraged ICANN and Registrars to work with law enforcement agencies to address their concerns on the misuse of the domain name system[55].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[56].

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

Other legal provisions

52 See http://www.iwf.org.uk/media/news.archive-2009.258.htm
53 See http://www.icann.org/
54 Every Commonwealth Government is eligible to join the GAC and attend its meetings
55 See http://gac.icann.org/system/files/Brussels-communique.pdf
56 See http://brussels38.icann.org/node/12448

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 aware of several other hazards which exist on the Internet and which are most likely to affect them e.g. exposure to age inappropriate but legal content, exposure to unscrupulous commercial practices, the risks 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 strategies for coping or dealing with these things, ideally how to avoid them altogether or, to increase their resilience, they need to know how to extricate themselves from difficult situations should problems nonetheless arise.

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 practice 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 education 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 education and awareness material available can vary enormously in quality 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[57]. The

57 See http://tinyurl.com/copinit (the authors of this paper were very closely involved in the preparation of the COP documents).

European Union's Safer Internet Programme[58], particularly the INSAFE[59] initiative and the TeachToday[60] website, are also tremendously valuable resources.

The ITU's COP initiative 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 Society[61]. 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.

58 See http://tinyurl.com/sipprog.
59 See http://tinyurl.com/insafehome.
60 See http://www.teachtoday.eu.
61 See http://www.itu.int/osg/csd/cybersecurity/WSIS/index.phtm.

appendix I

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

1. Antigua & Barbuda
2. Bahamas
3. Bangladesh
4. Belize
5. Cameroon
6. Dominica
7. Ghana
8. Grenada
9. Guyana
10. Kiribati
11. Lesotho
12. Malawi
13. Malaysia
14. Maldives
15. Mozambique
16. Namibia
17. Nauru
18. Nigeria
19. Pakistan
20. Rwanda
21. St. Kitts & Nevis
22. St. Lucia
23. St. Vincent & the Grenadines
24. Samoa
25. Sierra Leone
26. Singapore
27. Solomon Islands
28. Swaziland
29. Tanzania
30. Trinidad & Tobago
31. Tuvalu
32. Uganda
33. Zambia

appendix II

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

1. Gambia
2. Brunei
3. Kenya
4. Mauritius
5. Sri Lanka
6. India
7. Malta
8. Papua New Guinea
9. Seychelles

appendix III

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

1. Australia*
2. Barbados
3. Botswana
4. Canada
5. Cyprus
6. Jamaica
7. New Zealand
8. South Africa*
9. Tonga
10. United Kingdom
11. Vanuatu

*These countries meet all 5 criteria

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.

2010

Online Child Protection