

INTOLERABLE ACTS: AN ANALYSIS OF THE LAW RELATING TO ONLINE CHILD PORNOGRAPHY IN UGANDA

*by Rukundo Solomon**

1 Introduction

In recent years, Uganda has experienced considerable growth in the ICT sector. As of June 2015, the estimated number of Internet subscribers was 6 179 698 and internet users were 12 986 216.¹ By 2014 the RCDF had financed the setup of 76 Internet Points of Presence, 106 internet cafes and 78 Multi-Purpose Community Telecentres, 78 District web portals, 708 School ICT laboratories, and provided internet connectivity to over 300 projects across the country.² In Uganda computers are beginning to form an integral part of the social and economic life of the people. Computer based social media such as Facebook, WhatsApp and Twitter are increasingly getting more subscribers in Uganda, many of them being children.³ Internet penetration and legitimate usage has grown in tandem with internet abuses such as online child pornography. The risk of child sexual abuse in Uganda is considerably high with 77.7% of the primary school children and 82% of the secondary school students having experienced sexual abuse at school. 51% of victims were aged between 10 and 13 years, and 40.6% between 14 and 17.⁴ In 2013 alone 399 children were reported to have been trafficked internally while 230 children were trafficked across borders.⁵ It is in this already

* LLB (Hons) University of Dar es Salaam, Postgraduate Diploma in Legal Practice from the Law Development Centre in Uganda.

1 Ugandan Communications Commission, Annual Report 2014/2015.

2 The Rural Communications Development Fund (RCDF) run by the Uganda Communications Commission aims to ensure that quality communications services are accessed at affordable prices in rural and under-served areas: CIPESA 'State of Internet Freedoms in Uganda 2014: An Investigation into the Policies and Practices Defining Internet Freedom in Uganda' (2014).

3 R Kanyoro 'How social media has evolved in Uganda' <http://www.monitor.co.ug/arts/culture/Reviews/How-social-media-has-evolved-in-Uganda/-/691232/2771872/-/15q1foh/-/index.html> (accessed 5 February 2016).

4 The study was conducted by Winsor Consult LTD between 2011 and 2012. The sample was 40 primary schools and 10 secondary schools in 8 districts across 4 regions of Uganda: Government of Uganda, Ministry of Education and Sports 'Assessing child protection, safety & security issues for children in Ugandan primary and secondary schools' (July 2013).

5 Government of Uganda, Ministry of Internal Affairs 'Annual Report on the Trend of Trafficking in Persons in Uganda: 2013' (2014).

volatile environment that the internet appears as a catalyst for child abuse.

The availability and distribution of child pornography through the internet has been a social concern since the mid-1990s, when paedophiles started using this medium to share sexually explicit content to such an extent that one member of the Ugandan Parliament called it ‘the most powerful instrument for the paedophiles.’⁶ The making, viewing and distribution of child pornography takes place within a subculture⁷ that operates outside any particular state or legal jurisdiction and represents a new pattern of globalised crime and deviance.⁸ The increasingly cheaper accessibility of the internet has made pornography in general more readily available in Uganda, making computer-based pornography a significant crime.⁹ In the past, it was generally only family members or trusted friends, or perhaps clergy or teachers, who had private access to children. Now, the internet enables virtually anyone to communicate privately with children in their homes. Ironically, parents concerned about threats from ‘strangers’ may erroneously believe that their children are safer inside the home and on the computer.¹⁰ While a search on ‘child pornography’ on a web search engine, such as Google, would normally only produce sites campaigning against the availability of child pornography on the internet, child pornography thrives in channels devoted to it within the internet Relay Chat, ICQ environment and on peer to peer (P2P) file sharing systems¹¹ and can sometimes be found in ‘spam’ e-mails.¹²

6 Comments of Mr Awori in the Committee Stage of the Computer Misuse Bill reported in the Uganda Parliament Hansard on Tuesday, 29 June 2010. A 1986 Report of the US Senate Permanent Subcommittee on Investigations on Child Pornography and Paedophilia stated, ‘no single characteristic of paedophilia is more pervasive than the obsession with child pornography’ cited in J Clough *Principles of cybercrime* (2010) 5.

7 M Taylor & E Quayle *Child pornography: An internet crime* (2003) 126.

8 P Jenkins *Beyond tolerance: Child pornography on the internet* (2001) 5.

9 G Kamali ‘Pornography exported to Uganda’ http://www.newvision.co.ug/new_vision/news/1060278/-eur-pornography-exported-uganda-eur (accessed 31 January 2016); Uganda Law Reform Commission, ‘A Study Report on Electronic Transactions Law’ (2004) para 5.8(g).

10 Clough (n 6 above) 332; Increasingly children in Uganda are getting onto Social Networking sites such as Facebook, Twitter etc. which leave them vulnerable; Internet Society Uganda Chapter ‘Child online protection: An insight into legislation and practices in Uganda’ <http://internet.society.ug/uganda-igf/reports/#> (accessed 20 October 2016).

11 Y Akdeniz *Internet child pornography and the law: National and international responses* (2008) 7.

12 All Party Internet Group ‘“Spam”: Report of an inquiry by the All Party Internet’ para 21 <https://www.cl.cam.ac.uk/~rnc1/APIG-report-spam.pdf> (20 October 2016).

1.1 The foundations of the laws dealing with online child pornography in Uganda

In Uganda, the protection of children from pornography by parents, all citizens and the state, is mandated by the Constitution. Citizens have a duty to protect children from any form of abuse, harassment or ill treatment.¹³ It is the duty of parents to care for and bring up their children in a safe environment.¹⁴ Furthermore, under the Constitution, local laws and regional treaties, children are protected from social or economic exploitation and in particular activities that are harmful to their spiritual, moral or social development.¹⁵ International law imposes the duty on the State to take all appropriate national, bilateral and multilateral measures to prevent the exploitative use of children in pornographic performances and materials.¹⁶ The United Nations optional protocol on child pornography,¹⁷ to which Uganda is party, requires states to take all necessary steps to strengthen international co-operation in the prevention, detection, investigation, prosecution and punishment of those responsible for acts involving child pornography.¹⁸ The African Charter on the Rights of the Child further requires Uganda to protect the child from all forms of sexual exploitation and sexual abuse, and in particular to take measures to prevent the use of children in pornographic activities, performances and materials.¹⁹ The State's obligation to protect children from online sexual predators was noted by the European Court of Human Rights in *K.U. v Finland*,²⁰ where the Finnish government's failure to provide adequate legislative measures to facilitate investigations into child pornography was condemned by the court. In the South African case of *De Reuck v Director of Public Prosecutions*,²¹ it was stated that child pornography is seen as an evil in all democratic societies and that its criminalisation was a legitimate object.

Section 23 of the Computer Misuse Act 2011 (CMA) prohibits child pornography imposing a fine of 7, 200 000 Uganda shillings (roughly

13 Art 17(1)(c) of the Constitution of the Republic of Uganda 1995 (the Constitution).

14 Art 31(4) of the Constitution.

15 Art 34(4) of the Constitution; sec 8 of the Children Act ch 59; art 15 of the African Charter on The Rights and Welfare of The Child OAU Doc. CAB/LEG/24.9/49 (1990).

16 Art 34 of The United Nations Convention on The Rights of The Child.

17 Uganda acceded to the United Nations' Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography 2002 on 30 November 2001: Akdeniz (n 11 above) 219; <http://indicators.ohchr.org/> (accessed 06 January 2016).

18 Art 10(1) of the United Nations Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography 2002.

19 Art 27 of the African Charter on The Rights and Welfare of The Child OAU Doc. CAB/LEG/24.9/49 (1990).

20 (Application no. 2872/02) EctHR.

21 2004 (1) SA 406 (CC).

2000 US dollars) and or imprisonment for 15 years. The provision was restricted to *child* pornography so as to provide a special protection to children which would continue even if laws against adult pornography were ever relaxed.²² This provision in the CMA compliments a number of other obscenity laws in the country. Section 3 of the Press and Journalist Act²³ prohibits the publication of pornographic matters and obscene publications insofar as they tend to offend or corrupt public morals. Section 3 of the Prevention of Trafficking in Persons Act²⁴ provides that anyone who recruits a person through force or coercion for the purpose of engaging that person in pornography commits an offence.²⁵ Section 14 of the Anti-Pornography Act 2014, passed after the CMA, criminalises the production, trafficking, publishing, broadcasting, procuring, importing, exporting or in any way abetting pornography depicting the images of children and imposes an even stiffer fine of fifteen million shillings (about 4500 US dollars).²⁶ Regulation 5 of The Employment (Employment of Children) Regulations²⁷ prohibits children from being employed in the worst forms of child labour and regulation 2 defines the worst forms of child labour to include production of pornography or pornographic performances and the use of the internet to spread child pornography.²⁸

1.2 Definition of child pornography

It has been said that pornography is notoriously difficult to define, and child pornography no less so,²⁹ nonetheless the Parliament of Uganda has made at least two attempts at this.³⁰ Section 23(3) of the Computer Misuse Act defines child pornography as including pornographic material that depicts a child, a person appearing to be a child, and realistic images representing children, engaged in sexually suggestive or explicit conduct. This definition is a fairly broad

22 Parliament Hansard Tuesday, 29 June 2010. At the time the Act was passed, adult pornography was and still is illegal in Uganda.

23 Ch 105.

24 Prevention of Trafficking in Persons Act 7 of 2009.

25 Sec 3(4) of the Prevention of Trafficking in Persons Act provides that the consent of the victim of trafficking or if a child, the consent of his or her parents or guardians to the exploitation shall not be relevant.

26 Sec 14 of the Anti-Pornography Act.

27 SI 17 of 2012 (under secs 32, and 97 of the Employment Act 6 of 2006).

28 These are derived from the Convention concerning the International Labour Organisation Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour No.182 (1999): Government of Uganda, Ministry of Gender, Labour and Social Development, *National Child Labour Policy*, November 2006, para 1.1.3.

29 2004 (1) SA 406 (CC).

30 Computer Misuse Act 2 of 2011 and the Anti-Pornography Act 1 of 2014.

one capturing virtually any version of child pornography,³¹ and is similar to the one contained in the Council of Europe Convention on Cybercrime.³² The Anti Pornography Act, borrowing from the UN Convention,³³ defines child pornography as any representation through publication, exhibition, cinematography, indecent show, information technology or by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual enjoyment.³⁴ The definition in the Anti-Pornography Act was meant to be more comprehensive,³⁵ therefore the phrase ‘any representation’ could also cover textual material including cartoons, and drawings.³⁶ A child under Ugandan law is defined as any person below the age of 18.³⁷ This is in keeping with regional and international instruments.³⁸ In a recent ULRC study, the lowering of the age at which one ceases to be a child was vehemently rejected.³⁹ The Penal Code prohibits any sexual activity with a child; therefore consent of the child to the prohibited acts is irrelevant.⁴⁰

- 31 In the initial Bill the phrase read ‘visually depicts’ similar to that contained in the Convention on Cybercrime. However this was removed at Committee stage so as to make the provision wider capturing even audio depictions: Parliament Hansard Tuesday, 29 June 2010; United Nations Office On Drugs and Crime, Comprehensive Study on Cyber Security (2013) 101.
- 32 Art 10 of the Council of Europe Convention on Cybercrime European Treaty Series - No. 185 Budapest, 23.XI.2001 (Cybercrime Convention).
- 33 The United Nations’ Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography which came into force on 18 January 2002 defines child pornography in art 2(c) as ‘any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes’.
- 34 Sec 14(2) and sec 2 of the Anti-Pornography Act 2014.
- 35 During the passing of the Anti-Pornography Bill, the Chairperson, Committee on Legal and Parliament Affairs (Mr Stephen Tashobya) observed that there were some aspects of pornography control already covered in the legal regime prior to the Act but none of them comprehensively dealt with the vice. He cited as an example, the Computer Misuse Act 2 of 2011, catering for child pornography albeit not comprehensively: Parliament Hansard Tuesday, 19 December 2013.
- 36 *McEwen v Simmons* [2008] NSWSC 1292: Cartoon figures modelled on the children in an animated television series, ‘The Simpsons’, were engaged in sexual acts and this amounted to pornography.
- 37 Sec 2 of the Computer Misuse Act 2 of 2011; sec 2 of the Anti Pornography Act 1 of 2014.
- 38 Art 2 of the African Charter on The Rights and Welfare of The Child OAU Doc. CAB/LEG/24.9/49 (1990); Art 1 of the United Nations Convention on the Rights of the Child.
- 39 In a study conducted by the Uganda Law Reform Commission, the lowering of age of consent to below 18 years was opposed by medical practitioners with 60% of them advocating increasing it to 20 years. It was argued that below 18 years, a girl’s pelvic bones are not fully developed. Early pregnancies can lead to rupture of the uterus, damage of the urinary tract and Vesico Vagina Fistula (VVF). In addition, a girl is likely to be psychologically immature and incapable of sustaining marital pressure: Uganda Law Reform Commission, ‘Study Report on Marriage and Divorce in Uganda’ (2000) 56 & 59.
- 40 Sec 129 of the Penal Code Act Cap 120; in *Uganda v Kusemererwa* (Criminal case no: HCT-01-CR-SC-0015-2014) (2015) UGHCCRD 12 (25 November 2015) it was stated that a child is incapable of giving consent to sex.

It should be noted that all these definitions cover both real depictions as well as realistic and simulated representations. Computer Generated Images (CGI), as well as images of real persons above the age of 18 who appear to be a child under the age of 18, would therefore fall under these definitions. The inclusion of real images i.e. images of real children in the definition of child pornography, is directly aimed at protecting children from sexual abuse and exploitation. The children involved in the making of the pornography may suffer physical and mental injuries, and violations of their rights to dignity and privacy, therefore the prohibition of the making of such material is legitimate.⁴¹ There is an argument for criminalising the 'distribution' of CGI rather than their making, creation and possession as there is no evident direct harm perpetrated upon any children at the point of making of such pseudo-photographs.⁴² However, the justification for the inclusion of simulated representations is the concern that they may be used by paedophiles to groom and lure children for sexual activity, or encourage children to participate in sexual activity.⁴³ This is in contrast to the US position where it has been held by the Supreme Court that CGIs of child pornography are protected by the Constitution's free speech provisions.⁴⁴ Chief Justice Rehnquist's dissenting opinion in that Supreme Court case is of note as he argued that rapidly advancing technology would soon make it very difficult, if not impossible, to distinguish between pornography made with actual children and pornography made with simulated images of children.⁴⁵ Therefore the prohibition of simulated images is the most suitable way to deal with the vice.

2 Child pornography offences

2.1 Production

Section 23(1) (a) of the CMA criminalises the production of child pornography for the purposes of its distribution through a computer. To produce child pornography, someone has to assault a child, or pose

41 *R v Land* (1999) QB 65, 'The object is to protect children from exploitation and degradation. Potential damage to the child occurs when he or she is posed or pictured indecently, and whenever such an event occurs the child is exploited.'

42 Clough (n 6 above) 263.

43 S Sternberg 'The Child Pornography Prevention Act of 1996 and the First Amendment: Virtual Antitheses' (2001) 69 *Fordham Law Review* 2783 (also see <http://ir.lawnet.fordham.edu/flr/vol69/iss6/14>); Cybercrime Convention, Explanatory Report, para 93.

44 *Ashcroft v Free Speech Coalition* 535 U.S. 234 (2002).

45 As above.

a child in a sexualised way, and then make a photographic record of it.⁴⁶ In the South African case of *Kleinhans v S*,⁴⁷ a 74-year-old businessman befriended the complainants' families over a period of five years by assisting with various expenses such as school fees, groceries, clothing expenses, tuition and by supplying them with gifts; in one case even going so far as to purchase a motor vehicle for one of the complainants when she was older. He fitted out an unoccupied house which he owned with gymnasium equipment, ostensibly for use by himself and the complainants in the evenings. In truth this was just a cover for his activities and to assist him in procuring the complainants to pose for the pornographic pictures. The house was also fitted out with photographic equipment. A neighbour became suspicious of his regular arrival in a motor vehicle at the house in the afternoons and evenings, accompanied by one or more young girls sometimes dressed in school uniforms, and notified the police. He was found in the house with one of the complainants (aged between 13 and 14) who eventually told a policewoman that there were pictures of her on a memory stick which was found hidden on his person. In the pictures she was either naked or only partially clothed in a variety of poses, many of them highly suggestive, exposing at different times her breasts, vagina, buttocks and also at times the inner portions of her vagina and anus. In certain photographs, vibrators were placed on or in her vagina. A total of 86 such photographs were found on a memory stick hidden on his person. He was convicted of producing child pornography. Similarly in *S v Stevens*,⁴⁸ the appellant removed the undergarments of the two young girls aged five years at the time while they were sleeping and took photographs with more active participation on their part, and in certain instances placing his finger on the vagina of the two young girls. Some 71 photographs of the children were taken. The photographs were not distributed and were used by the appellant only for his own sexual gratification. He was convicted and sentenced to 6 years imprisonment. Pornography can be produced even without the knowledge of the child as was the case in *M v S*,⁴⁹ where the 14-year-old complainant discovered that the appellant had installed a hidden video camera that could record images of her when using the bathroom and shower. Research has found that whether it is for private use or commercial distribution, a parent, guardian, or family friend is often responsible for the production of child pornography.⁵⁰

46 Taylor & Quayle (n 7 above) 21.

47 *Kleinhans v S* 2014 (2) SACR 575 (WCC).

48 *S v Stevens* (CA&R54/07) [2007] ZAECHC 53 (22 June 2007).

49 2013 (2) SACR 111 (SCA).

50 Taylor & Quayle (n 7 above) 22.

Controversially, in the United Kingdom, it has been held that the mere downloading of child pornography can amount to ‘making’ it. In *R v Bowden*⁵¹ Jonathan Bowden, a schoolteacher, downloaded photographs containing indecent images of young boys from the internet and printed out and stored them on computer discs for his personal use. He was charged with making an indecent photograph. The prosecution argued that a person who either downloaded images on to disc or who printed them was making them as the law was not only concerned with the original creation of the images, but also their proliferation. Therefore downloading or printing the images was to create new material. The Court of Appeal accepted this argument holding that the words ‘to make’ had to be given their natural and ordinary meaning which in this context, relying on the Oxford Dictionary, meant ‘to cause to exist; to produce by action, to bring about.’ This applied not only to original photographs but also to negatives, copies of photographs and data stored on a computer disc.⁵² This interpretation was accepted by the same court in *R v Graham Westgarth Smith and Mike Jayson*⁵³ where the court stated that ‘the act of voluntarily downloading an indecent image from a web page on to a computer screen is an act of making a photograph or pseudo-photograph.’ If this interpretation is adopted in Uganda, then the mere downloading of child pornography would amount to producing it contrary to this sub section. This interpretation would be suitable bearing in mind that ‘even the young inexperienced amateur who downloads one image for his or her personal gratification does a significant criminal act which adds to the scale of human misery because, if there was no market for these images children would not be degraded producing them.’⁵⁴

2.2 Offers or Makes Available

Section 23(1) (b) of the CMA prohibits the offering or making available of child pornography through a computer. ‘Offering’ is intended to cover soliciting others to obtain child pornography, and implies that the person offering the material can actually provide it. ‘Making available’ includes publishing, showing and advertising.⁵⁵ ‘Making available’ is intended to cover the placing of child pornography on websites, and the use of hyperlinks to facilitate access to child

51 *R v Bowden* (2000) 2 All ER 418.

52 However, it appears that where the defendant is unaware that the download is taking place as is the case when files are automatically saved in the cache, there is no making involved: *Atkins & Goodland v Director of Public Prosecutions* (2000) 2 All ER 425.

53 *R v Graham Westgarth Smith and Mike Jayson* [2002] EWCA Crim 683.

54 *R v Toomer and others* [2001] 2 Cr App R(S) 30, Lexis UK CS 1705, para 6.

55 Clough (n 6 above) 287.

pornography.⁵⁶ This therefore covers websites and chat rooms where child pornography is made available. In *US v Rowe*,⁵⁷ the defendant posted in an internet chat room, known as 'preteen00,' showing the software program he used, the password needed to access the file server and that he had pictures of pre-teen boys and girls and that a person wishing to access the images would have to read the rules of use and upload an equivalent number of images to his computer. A search warrant was subsequently executed and 12,000 child pornographic images and videos were found on the defendant's computer. The court rejected the defendant's argument that the posting did not constitute an advertisement as it did not specifically refer to pornography, but rather only referred to pictures of prepubescent boys and girls. It was held that there was no doubt that the defendant's posting knowingly offered or sought images depicting minors engaged in sexually explicit conduct. Even a password protected website would still amount to making available. In *R v Fellows and Arnold*⁵⁸ it was held that placing material on the internet for downloading, even if it is subject to a password, was to 'publish' within the terms of the Obscene Publications Act 1959 (UK).

2.3 Distribution

Distribution or transmission of child pornography through a computer is prohibited by section 23(1) (c) of the CMA. 'Distribution' which involves the active dissemination of child pornography⁵⁹ is inapplicable to the process of downloading images where the recipient is the end-user.⁶⁰ It is, however, clearly applicable to the process of sending images over computer networks by e-mail or in chat rooms, and to the uploading of files onto bulletin boards.⁶¹ A person is to be regarded as distributing child pornography if he parts with possession of it to, or exposes or offers it for acquisition by, another person. Thus sending pornography as an attachment to an e-mail message, or posting to a newsgroup, or publishing on a website, or making it available for sharing or download through a P2P (peer to peer) network would qualify as distribution.⁶² Transmission ordinarily

56 Cybercrime Convention, Explanatory Report Para 95; *Universal City Studios v Reimerdes*, 111 F Supp 2d 294, 325 (SD NY 2000); *Universal Music Australia Pty Ltd v Cooper* (2005) 150 FCR 1 (Australia); A supporter of the hacker group Anonymous published DDoS (Distributed Denial of Service) cyber-attack links to UK Home Office and Home Secretary Theresa May websites on Twitter and was convicted; Stoke & Staffordshire 'Mark Johnson guilty of 'crippling' Home Office cyber-attack' <http://www.bbc.com/news/uk-england-stoke-staffordshire-29958425> (accessed on 12 February 2016).

57 *US v Rowe* 414 F 3d 271 (2nd Cir 2005) (USA).

58 *R v Fellows and Arnold* (1997) 2 All ER 548 at 558-9.

59 Cybercrime Convention, Explanatory Report para 96.

60 Clough (n 6 above) 293.

61 As above.

62 Akdeniz (n 11 above) 7.

means to cause (a thing) to pass, go, or be conveyed to another person, place, or thing. The offence is therefore well suited to the sending of child pornography via a computer system, whether by uploading, e-mail, peer-to-peer or any other form of electronic communication.⁶³ In *R v Hyett*⁶⁴ the defendant admitted that she encouraged and instructed her daughter of 13 years of age to accede to the requests of a man to see her breasts through a chat room conversation despite her protests. The defendant and her partner were convicted of distributing an indecent photograph of a child.

2.4 Procuring

Section 23(1) (d) of the CMA criminalises the procuring of child pornography through a computer. The term ‘procuring for oneself or for another’ means actively obtaining child pornography, e.g. by downloading it.⁶⁵ Procuring includes: accessing, causing to transmit, receiving and requesting for child pornography.⁶⁶ This offence serves to compliment the possession offence in section 21(1)(e) as the traditional legal notions of possession may prove problematic in cyberspace due to concepts of physical custody and control which evolved in the context of tangible items.⁶⁷ An example of the possession offence’s limitation is viewing a video online without deliberately storing it on the computer. In such circumstances actual possession may be difficult to prove though it is clearly established that the defendant did in fact view child pornography. Internet records, both on the defendant’s computer and in the records of ISPs, may provide evidence that the defendant in fact accessed child pornography, irrespective of whether it was viewed, saved to disk or otherwise dealt with. Such conduct falls under ‘procuring,’ which is intended to deal with a person who actively obtains child pornography; for example, by downloading it, whether for himself or another.⁶⁸

2.5 Possession

Section 23(1)(e) of the CMA states that a person who unlawfully possesses child pornography on a computer, commits an offence. The word ‘unlawful’ was added to cater for the possibility of legitimate possession such as law enforcement, research and genuine scientific purposes.⁶⁹ A defendant may be in possession of an item in one of two

63 Clough (n 6 above) 294.

64 *R v Hyett* (2001) EWCA CRIM 669.

65 Cybercrime Convention (n 59 above) para 97.

66 Clough (no 6 above) 296.

67 As above.

68 As above.

69 Parliament Hansard Tuesday, 29 June 2010.

ways. The first is the obvious one where the item is in the physical custody or control of the defendant. The second, also called ‘*de facto* custody,’ is where the item is in a place where he may go, without physical bar, in order to obtain such manual possession.⁷⁰ An example of the first is in the US case of *US v Tucker*⁷¹ where by means of forensic examination 27,000 images, an estimated 90-95 percent of which were child pornography, were recovered from the ‘Internet Explorer’ cache file and the temporary internet files in the computer hard drive’s ‘recycle bin.’ Images had been viewed but the storage had been automatic and not necessarily deliberate. The defendant therefore denied being in possession of the images on the basis that he could not be found to be in possession of something which he didn’t ‘download, copy or intentionally store.’ This argument was rejected as the defendant clearly exercised control over the images in a number of ways. He could enlarge or otherwise manipulate them, he could print and he could copy them. In particular, his control over the images automatically stored in the cache was illustrated by his practice of deleting them. However, in *Atkins & Goodland v DPP*⁷² the offending images were contained in the cache memory of the defendant’s machine but expert evidence was submitted which indicated that most computer users are unaware of the operation of the cache memory feature on their machines. It was held that the offence of possession was not committed unless the defendant knew that he had, or had once had, the photographs in his possession. Accordingly, an accused could not be convicted where, as in this case, he could not be shown to have been aware of the existence of a cache of photographs in the first place. *De facto* custody applies in situations where the defendant has hidden the pornography effectively so that he can take it into his physical custody when he wishes and where others are unlikely to discover it except by accident.⁷³ It would apply to remote storage of digital files such as where the accused uploads material to a local server or ISP. Where the defendant is able to copy, delete or otherwise manipulate such files remotely, then he or she may be said to be in possession of those files, for example where the images are found on a website maintained by the defendant.⁷⁴

Where the defendant has deleted an image, and believes it to have been removed from the computer, the fact that the defendant is mistaken, or that other people may be aware that such images may

70 Clough (no 6 above) 302.

71 *US v Tucker* 150 F Supp 2d 1263 (D Utah 2001).

72 *Atkins & Goodland v DPP* [2000] 2 All ER 425.

73 Clough (no 6 above) 310.

74 As above.

be recovered through technical means, is irrelevant to the subjective knowledge of the defendant.⁷⁵ In *R v Porter*⁷⁶ the defendant had been charged with possession in respect of some 3000 still images and 40 movie files. However, for the period in respect of which the charge related, it was conceded that the images and files had been deleted and were viewable only in thumbnail format, or were only present in the computer cache. The court held that if a person cannot retrieve or gain access to an image he no longer has custody or control of it and therefore can not be said to be in possession. However, a defendant could be found to remain in control of deleted files, where, due to his level of technical skill and possession of the necessary software, he can easily retrieve the files.

2.6 Unsolicited photographs

Where a photograph or pseudo-photograph is sent to the defendant without any prior request by him or on his behalf, this does not amount to production, procuring, or possession provided the defendant does not keep it for an unreasonable time.⁷⁷ The issue of reasonableness in a matter is decided on the facts of any individual case.⁷⁸ There are at least three new ways in which individuals might become unintentional recipients of child pornography in computer-based transactions: through unsolicited 'spam' e-mails, pop-up advertisements during legal internet searches,⁷⁹ and viruses.⁸⁰ Further, with a shared computer or e-mail account, images and files may be placed on a computer or e-mail account without the knowledge or consent of one of the users. Although the CMA does not have knowledge of the images as a *mens rea* requirement, courts have held that a *mens rea* requirement will be read into criminal statutes⁸¹ and therefore a requirement that the defendant know that the images relate to child pornography can be presumed.⁸² In *R v Graham Westgarth Smith & Mike Jayson*⁸³ it was held that a person is not

75 As above.

76 *R v Porter* [2006] EWCA Crim. 560.

77 Akdeniz (n 11 above) 37.

78 As above.

79 Akdeniz (n 11 above) 37; 'Within the context of the Internet, presumably, the courts would treat pop-up websites as unsolicited, and if certain websites trigger pop-up advertisements involving indecent images of children then this could be treated as unsolicited if there was no further intention to store the advertisement images by the suspect.'

80 In *United States v Miller* 527 F.3d 54 (3d Cir. 2008) the court relied on expert testimony to conclude that 'a person may come to knowingly possess a computer file without ever knowingly receiving it.' Cited in DM Rice 'Note: Child pornography, the internet, and the challenge of updating statutory terms' (2009) 122 *Harvard Law Review* 2215-2216.

81 *Sweet v Parsley* [1970] AC 132; *Uganda v Dr. Richard Ndyomugenyi & 2 others* (CR.SC 003 OF 2010) ((CR.SC 003 of 2010)) (2010) UGHC 49 (31 August 2010).

82 Rice (no 80 above) 2217.

83 *R v Graham Westgarth Smith & Mike Jayson* (2002) EWCA Crim. 683.

guilty of an offence of ‘making’ or ‘being in possession’ of an indecent photograph contained in an email attachment if, before he opens the attachment, he is unaware that it contains or is likely to contain an indecent image. Once he realises what the contents are, the defendant would have to delete the illicit files within a reasonable time. In *R. v Collier (Edward John)*⁸⁴ the defendant had in his possession tapes and CD-ROMs containing indecent images but maintained that he never suspected that the material would include indecent images of children. The court stated that it would seem wrong to penalise a person for having images which he proves that he has not seen when he also proves that he did not know or have reason to suspect that they were indecent images of a child. If the defendant proves that he had not seen the photograph and did not know and had no cause to suspect that it was an indecent photograph of a child, he must be acquitted of the possession offence.

2.7 Showing pornography to children

Section 23(2) of the CMA states that a person who makes available pornographic materials to a child commits an offence. This criminalises the showing of any kind of pornographic material to a child whether it involves adults or children.⁸⁵ This, as seen above, is in keeping with the Constitution that guarantees the protection of children from social exploitation that is harmful to their mental, spiritual, moral or social development.⁸⁶ It protects children from a form of online grooming⁸⁷ whereby they are shown pornography involving children to encourage them to participate in sexual behaviour at a young age. For example in the Canadian case of *R v VH*⁸⁸ the defendant used child pornography downloaded from the internet in an attempt to persuade his twelve-year-old daughter that incest was normal. In the South African case of *Botha v S*⁸⁹ the court noted that child pornography ‘is potentially harmful because of the attitude to child sex that it fosters and the use to which it can be put in grooming children to engage in sexual conduct.’ In *M v S*⁹⁰ the defendant showed pornography to the 14-year-old complainant prior to engaging in sexual acts with her. Finally in *Print Media South Africa and Another v Minister of Home Affairs and Another*⁹¹ the

84 *R v Collier (Edward John)* (2004) EWCA Crim. 1411.

85 Parliament Hansard Tuesday, 29 June 2010.

86 Art 34(4) of the Constitution of the Republic of Uganda 1995.

87 This is the intentional proposal, through information and communication technologies, by an adult to meet a child for the purpose of committing an offence: United Nations Office On Drugs and Crime, Comprehensive Study on Cyber Security (n 31 above) 103.

88 *R v VH* (2001) 10 VR 234.

89 (A163/2014) (2015) ZAFSHC 34 (26 February 2015).

90 (657/12) (2013) ZASCA 43 (28 March 2013).

91 2012 (12) BCLR 1345 (CC).

Constitutional Court of South Africa held that protection of children from exposure to inappropriate materials was a legitimate object to be pursued by the state through her laws.

The provision, however, does not adequately cater for the initial stages of online child grooming which are less explicit. At its initial stage, grooming will involve socialisation through which an offender seeks to interact with a child, possibly sharing their hobbies and interests in an attempt to gain trust in order to prepare them for sexual abuse.⁹² Social networking sites in particular may facilitate this process and children easily share information thereon.⁹³ The internet allows for an almost instant sense of intimacy between people who have never met. Some people will quickly tell a stranger very intimate thoughts as the fact that they are not physically near the person and cannot see him or her lowers inhibitions. Over time children or adolescents can come to believe that the person they have been communicating with actually cares about them.⁹⁴ Groomers often target vulnerable children lacking in confidence, with low self-esteem or who are emotionally deprived. The fact that some victims of child pornography may be willing participants does not make them any less of victims.⁹⁵ It is worth noting that a number of countries have created legislation that deals specifically with this practice.⁹⁶ An illustration of this practice in an offline environment is in the South African case of *Ravi v Chetty*⁹⁷ where a teacher graphically described certain sexual acts to a 13-year-old pupil then proceeded to sexually assault her.

2.8 Abetment

Section 21(1) of the CMA provides that one who abets another in committing an offence under the Act is treated as having committed that offence and is therefore liable on conviction to the punishment prescribed for the offence. This reiterates the provisions of section 19 the Penal Code Act⁹⁸ which provides that every person who aids or abets in the commission of an offence commits that offence.⁹⁹

92 J Davidson 'Legislation and policy: Protecting young people, sentencing and managing, internet sex offenders' in J Davidson & G Peter (eds) *Internet child abuse: Current research and policy* (2011) 9.

93 T Jon 'Policing social networking sites and online grooming' in J Davidson & G Peter (eds) *Internet child abuse: Current research and policy* (2011) 127.

94 MM Ferraro *et al Investigating child exploitation and pornography: The internet, the law and forensic science* (2005) 55.

95 S Ost *Child pornography and sexual grooming: Legal and societal responses* (2009) 9.

96 The Sexual Offences Act (2003) in England and Wales, and Northern Ireland, the Protection of Children and Prevention of Sexual Offences Act (2005) in Scotland the Crimes Amendment Act (2005) in New Zealand include offences dealing with this. See Davidson (n 92 above) 3.

97 *Ravi v Chetty* Case No AR 377/2014 (South Africa).

98 Ch 120.

Abetment is where some assistance or encouragement is voluntarily done with the knowledge of the circumstances constituting the crime and it is irrelevant that the assistance was not given with the motive of encouraging the crime.¹⁰⁰ One can be convicted of abetting in the commission of an offence provided he had the necessary *mens rea* i.e. that he participated in the commission of the offence in the full knowledge that it was an offence.¹⁰¹ In *The State v SV & FH*¹⁰² one of the accused, the mother to the victim was convicted of assistance in the creation and production of child pornography. She recorded and participated in the sexual abuse of her daughter with her partner. However, where the offence was complete before the abetment, the abettor cannot be made liable under this section.¹⁰³ Therefore anyone who assists in the commission of any of the child pornography offences commits the same offence.

2.9 Attempts

Section 21(2) of the CMA provides that any person who attempts to commit any offence under the Act commits that offence and is liable on conviction to the punishment prescribed for the offence. An attempt is defined as when a person, intending to commit an offence, begins to put his or her intention into execution by means adapted to its fulfilment, and manifests his or her intention by some overt act, but does not fulfil his or her intention to such an extent as to commit the offence, he or she is deemed to attempt to commit the offence.¹⁰⁴ The circumstances preventing the commission of the offence are immaterial except for purposes of sentencing;¹⁰⁵ therefore a thwarted attempt; a failed attempt and an impossible attempt all fall foul of this section.¹⁰⁶ The definition of attempt in the CMA mirrors precisely that contained in the Penal Code Act.¹⁰⁷ In the law of attempts, the mental element is crucial: it is the intention of the actor that the substantive offence be committed which makes his conduct potentially dangerous and justifies the intervention of the criminal law before any concrete harm has been done. However, it is very important to remember that there is no liability for merely planning alone, to commit an offence. There must be an overt act for an accusation of attempt to succeed.¹⁰⁸ In other words, merely having

99 *Uganda v Kankiruhó James & Another* (1996) I KALR 70 (HCCC) & *Kalange Steven v Uganda* (1996) VI KALR 107 (HCCR).

100 *Uganda v Mugenyi Godfrey & Another* (1994) II KALR 76 (HCCR).

101 *Ali Islam v Republic* [1967] 1 EA 246 (High Court of Tanzania at Dar-es-Salaam).

102 *The State v SV & FH* Case No. CC82/2014 (South Africa).

103 *Njoroge v Republic* [1969] 1 EA 17 (High Court of Kenya at Nairobi).

104 Sec 22(1) of the CMA.

105 Sec 22(2) of the CMA.

106 J Herring *Criminal law* (2011) 346.

107 Sec 386(1) of the Penal Code Act Ch 120.

108 Sec 22(1).

a desire to procure child pornography is not an offence. The accused must have gone a step further in his efforts to fulfil his wicked designs such as requesting for or attempting to download child pornography. The CMA only departs from the Penal Code by providing that one who attempts to commit an offence under the Act is liable on conviction to the punishment prescribed for the offence.¹⁰⁹ In effect, one who merely attempts to engage in a child pornography offence is treated as the same as one who in fact succeeds in doing the act. The severity of the punishment in relation to a mere attempt can be justified by the need for deterrence of computer related crimes.¹¹⁰ Though not decided on the law of attempts, the Canadian case of *R v Daniels*¹¹¹ is instructive. In this case, the accused was downloading child pornography but terminated the download before it was complete. On the evidence, there was no doubt that the defendant was aware that he was ordering child pornography as he had to read a graphic description before proceeding to download. It was, however, impossible to establish how much of the image appeared on the defendant's screen, and none of the requested images were found on the defendant's computer. It was held that once the downloading had begun, absent some computer malfunction, Daniels had complete control in deciding how much of the image would be displayed on the computer screen. To be in possession of child pornography, it is not necessary for the individual to have viewed the material.

3 Liability of internet service providers

The main function of internet Service Providers (ISPs) is the commercial provision of internet access services such as dialup and broadband to the online users. It is not possible (especially for home users) to access the internet without the services of an ISP, and therefore the role of an ISP is crucial.¹¹² ISPs may be content providers themselves, offering content to customers ranging from small scale such as the provision of a web page with information relevant to their customers to creating and providing content for their customers such as news, sports and entertainment.¹¹³

Under the Electronic Transactions Act 2011 of Uganda, an ISP is not subject to civil or criminal liability in respect of third-party material to which it merely provides access.¹¹⁴ The Act further states that an ISP is not liable for damage incurred by the user if the ISP does

109 Sec 21(2).

110 United Kingdom, Law Commission, Computer Misuse, Working Paper No. 110 (1988) para 2.15.

111 *R v Daniels* (2004) NLSCTD 27 (Supreme Court of Newfoundland and Labrador).

112 Akdeniz (n 11 above) 227.

113 As above.

114 Sec 29 of the Electronic Transactions Act 4 of 2011.

not have actual knowledge of the infringing material or circumstances from which the infringing activity is apparent and does not receive a financial benefit directly attributable to the infringing activity.¹¹⁵ These provisions on their own would in effect immunise ISPs with respect to 'third-party content' that travels through their servers but not any material the ISPs develop or create entirely by themselves. However, although an ISP is not obliged to monitor the data which it transmits or stores,¹¹⁶ it is obliged to remove or disable access to the reference or link to the data message or activity within a reasonable time after being alerted to it otherwise it loses its immunity.¹¹⁷ The declared rationale for such an approach is that if ISPs were to be held liable for all content to which they provide access, then they would be less likely to offer such services, which would be to the detriment of the development of e-Commerce.¹¹⁸ This is similar to the approach used in the US as seen in the case of *Doe v America Online, Inc.*¹¹⁹ where America Online (AOL) faced criminal prosecution following allegations by the mother of an 11-year-old that AOL had created 'a home shopping network for paedophiles.' According to the lawsuit brought by the mother, one AOL subscriber, Ron Russell, allegedly used the service to sell images of sexual acts involving himself, her 11-year-old son and two other boys he had befriended. In its defence, AOL argued that all Doe's claims were barred by laws which stated that they were not liable for their content. It was held that AOL was not liable as making it liable would treat it as the publisher or of those communications. Second, it would subject AOL to principles of liability that govern traditional publishers (such as newspapers and magazines) but that do not govern entities (such as telephone companies) that provide a service over which numerous third parties may communicate with one another. Third, it would impose on AOL, as a matter of law, a standard of care that would require AOL to monitor, screen and censor the great volumes of information transmitted over its system by third parties which might not be practicable.

Section 29(2) of the CMA limits the immunity of the ISP stipulating that the ISP has an obligation which is imposed by law or a court to remove, block or deny access to any material. One such law is section 17 of the Anti Pornography Act which states that ISPs which do not use

115 Sec 30 of the Electronic Transactions Act.

116 Sec 32 of the Electronic Transactions Act.

117 Sec 30(d) of the Electronic Transactions Act.

118 Draft East African Framework for Cyber Laws (2008), para 2.1.5.

119 *Doe v America Online, Inc.* 25 Media L. Rep. (BNA) 2112; 1997 WL 374223 (Fla. Cir. Ct. 26 June 1997); Case No. 97-2587 (Fourth District Court of Appeal, Fla., 14 October 1998).

the procedures set by the Pornography Control Committee,¹²⁰ a body created under that Act, and thereby permit any pornographic content through the service are liable to a fine of ten million shillings or five years imprisonment. Therefore ISPs have the obligation of following the procedures established by the committee so as not to fall foul of this section.

4 Conclusion

As seen from the above analysis, the legal regime to combat online child pornography is, with a few shortfalls, largely adequate and efficient. However, there are some issues it does not address satisfactorily. For example, as discussed above, the provisions do not adequately cater for the initial stages of online child grooming. Further, the provisions clearly do not anticipate a scenario where children themselves voluntarily send images of themselves to each other, a practice popularly known as ‘sexting’. This is a growing habit in some jurisdictions and ought to be addressed by the law.¹²¹ As it stands now children engaging in sexting would be charged with the offence of child pornography.¹²² Further, the blanket immunity given to the ISPs is questionable. Though significant inroads are made against the immunity by the CMA and the Anti Pornography Act, these still leave the exact extent and nature of ISP liability subject to some debate. Internet service providers control the gateway through which child pornography and other internet pests enter and re-enter the public computer system. They should therefore bear some responsibility for stopping these pests before they spread and for helping to identify individuals who originate them in the first place.¹²³

Nonetheless, great effort has been made in ensuring the enforceability of the provisions of the CMA. The Electronic

120 The members of the Pornography Control Committee were appointed in April 2016 however they claim that they are unable to fulfill their duties due to limited funding: Anonymous ‘Pornography control committee named’ http://www.newvision.co.ug/new_vision/news/1422110/anti-pornographic-committee-named (accessed 09 June 2016); B Musinguzi ‘Uganda: Anti-Pornography Committee Redundant’ <http://www.monitor.co.ug/News/National/Anti-pornography-committee-redundant/688334-3304124-l07jex/index.html> (accessed 9 August 2016).

121 T Crofts & M Lee ‘“Sexting”, children and child pornography’ (2013) 35 *Sydney Law Review* 85.

122 In jurisdictions where this practice is common among young people there have been many reports of teenagers being prosecuted for child pornography offences (Crofts & Lee, 2014). Sec 88 of the Children Act Ch 59 provides that the minimum age of criminal responsibility shall be twelve years. Therefore children of age twelve and above who engage in the practice are liable to prosecution.

123 DG Lichtman & E Posner ‘Holding internet service providers accountable’ <http://ssrn.com/abstract=573502> or <http://dx.doi.org/10.2139/ssrn.573502> (accessed 16 July 2016).

Transactions Act and the Regulations thereunder provide a procedure through which infringing material can be reported to ISPs.¹²⁴ As part of the efforts to combat child pornography, the Government of Uganda and internet Watch Foundation (IWF) have launched a Portal for Ugandan citizens to report child sexual abuse images and videos.¹²⁵ There is also a provision for reporting child abuse online on the Internet Society-Uganda Chapter Website¹²⁶ and on the website of Ministry of Gender, Labour and Social Development.¹²⁷ NITA collaborated with the internet Society Uganda to develop the Online Safety Educational Toolkit to educate students on how to recognise potential internet risks and empower children to help prevent themselves from being exploited online, or to report possible victimisation to a trusted adult.¹²⁸ A multi-sectoral working group on Child Online Protection has been put in place centred at the Ministry of Internal Affairs with the main purpose of educating all categories of internet users including children on responsible use as well as creating awareness among key stakeholders and duty bearers.¹²⁹

124 Sec 31 of the Electronic Transactions Act and reg 19 of the Electronic Transactions Regulations SI 42 of 2013.

125 NITA 'Uganda launches Portal with IWF' <http://www.nita.go.ug/media/uganda-launches-portal-iwf> (accessed 03 February 2016). The portal used to report is <https://report.iwf.org.uk/ug/>.

126 Internet Society-Uganda Chapter website is <http://Internetsociety.ug/>.

127 Ministry of Gender, Labour and Social Development website is <http://www.mglsd.go.ug/blog/report-online-child-sexual-abuse.html>.

128 Internet Society Uganda Chapter 'Online Safety Education Toolkit for Young People in Uganda' www.nita.go.ug/sites/default/files/publications/COP-Toolkit-ISOC-UG.PDF (accessed on 3 February 2016).

129 L Mbonimpa 'Why you should care for a better internet' http://www.newvision.co.ug/new_vision/news/1416673/care-internet (accessed 18 February 2016).