Reforming the law on child sexual abuse images

Graeme Horsman

Abstract

In seeking sexual gratification, an individual does not have free reign to seek or produce material of any type with many jurisdictions having sought to legislate on the forms of content that are legally acceptable. As a result, in England and Wales it is illegal to take, make, publish, distribute or possess images depicting child sexual abuse (IDCSA). IDCSA are now arguably considered in today's society as one of the worst forms of material that can be characterised (albeit incorrectly) as pornographic. Yet despite legislation directly targeting the regulation of IDCSA being in force since the Protection of Children Act 1978, images of this type are still considered to be prevalent, arguably due to the Internet and developments in digital technologies. Now, many IDCSA exist in a digital form on digital devices as opposed to tangible photographs. This transition in form has given rise to a complex area of legal debate, particularly in the areas of establishing possession of digital IDCSA, a focus of this work.

This thesis provides a discussion of the harm caused by IDCSA, both to the child depicted and to society, with a chronological analysis of laws surrounding IDCSA in England and Wales presented. The thesis then focuses on the offence of possession of IDCSA and the elements of the current test of possession are examined. Key areas of interest are highlighted in regards to the possession offence, including IDCSA found in the deleted areas of a device, the Internet cache and the impact of encryption. Finally conclusions are drawn and reform suggestions have been proposed, including the implementation of a new offence of 'accessing' IDCSA.

Reforming the law on child sexual abuse images

Graeme Horsman

MJur Thesis

Durham Law School, University of Durham

2016

Contents

List of Abbreviations

Bulletin Board Systems	BBS
Combatting Paedophiles Information Networks in Europe Centre	COPINE
Criminal Justice Act 1988	CJA88
Criminal Justice and Public Order Act 1994	CJPO94
Digital Forensics	DF
Digital storage media	DSM
Draft Investigatory Powers Bill	DIPB
Images Depicting Child Sexual Abuse	IDCSA
Indecent Images of Children	IIoC
Internet Watch Foundation	IWF
Obscene Publications Act 1959 & 1964	OPA
Operating System	OS
Protection of Children Act 1978	PCA78
Regulation of Investigatory Powers Act 2000	RIPA
Volume shadow copy	VSC

Chapter 1

The Development of Pornography and Images Depicting Child Sexual Abuse

1 Introduction

This thesis provides a discussion of child sexual abuse imagery laws in England and Wales, with a focus maintained on analysing the offence of possession. The thesis aims to assess the complexity of the current test of possession for this form of imagery. A discussion of digital forensic evidence is provided to emphasise current difficulties surrounding the application of current possession laws. The full structure of the thesis is provided in section 1.5. The remainder of Chapter 1 will introduce discussions surrounding pornography and child sexual abuse imagery, first tackling the use of appropriate terminology for addressing this content. The impact of technology upon the production and distribution of child sexual abuse imagery will be highlighted, with both pre and post Internet positions considered. The problem posed by illegal imagery is also considered, with particular focus on those who possess this material.

It is estimated that globally, the pornographic industry is worth 97 billion dollars[1]. In addition, around 14% of all Internet searches are conducted for the purpose of finding sexual content hosted online[2]. Although pornography has existed in varying forms for centuries, it is only now with the substantial development of the 'porn industry' along with increased media coverage and an unprecedented demand for consumer consumption[3], that society is now more conscious of its existence[4]. What was once predominantly confined in the 1960s', 70s' and 80s' to written publications accessible only in specialist underground

[1] C Morris, 'Porn Industry Feeling Upbeat About 2014' *NBC News* (U.S., 14 January 2014) <http://www.nbcnews.com/business/business-news/porn-industry-feeling-upbeat-about-2014-n9076> accessed 12 September 2014

[2] M Ward, 'Web porn: Just how much is there?' *BBC News* (London, 1 July 2013) <http://www.bbc.co.uk/news/technology-23030090> accessed 12 September 2014

[3] N. M. Lambert, S. Negash, T. F. Stillman, S. B. Olmstead, & F. D. Fincham, 'A love that doesn't last: Pornography consumption and weakened commitment to one's romantic partner' (2012) 31 Journal of Social and Clinical Psychology 410, 410

[4] C. A. MacKinnon, 'Pornography, civil rights, and speech' (1985) 20 Harv. CR-CLL Rev. 1

outlets[5], pornographic content has now found its way into the homes of millions throughout Europe and the United States (US). The volume of pornographic material in circulation has now significantly increased; mainly due to the wide spread availability and use of affordable personal computers and media recording devices[6], coupled with the development of fast and reliable Internet services. As a result, pornography and sexualised images now feature in almost all aspects of society.

Pornographic content is defined in the Oxford dictionary as "material containing the explicit description or display of sexual organs or activity, intended to stimulate sexual excitement"[7]. Expanding on this, the Williams Committee report states that "a pornographic representation is one that combines two features: it has a certain function or intention, to arouse its audience sexually, and also a certain content, explicit representations of sexual material (organs, postures, activity, etc). A work has to have both this function and this content to be a piece of pornography"[8]. The type of material that constitutes pornography is subjective to each individual viewer. What constitutes pornography differs depending on the varying interests of different social groups[9] and varied cultural norms[10], with Lindgren[11] suggesting that these factors have created a significant difficulty when attempting to provide a global classification. This has led to what can be best described as an assorted range of material, often categorised under the umbrella term of pornography, surfacing across Europe and the US. Further, increasing Internet usage has generated an incoming wave of "hard-core pornography including: buggery, cunnilingus, urination, and bondage, etc., sanitised by the terms "explicit sex", "adult entertainment" and "human sexuality""[12]. Extreme examples also include, but are not limited to content such as, necrophilia, the sexual intercourse or attraction to corpses[13] and snuff films, "a pornographic film or video

[5] J. Wolak, K. Mitchell, & D. Finkelhor, 'Unwanted and wanted exposure to online pornography in a national sample of youth Internet users' (2007) 119.2 Pediatrics 247

[6] F. D'Orlando, 'The demand for pornography' (2011) 12 Journal of Happiness Studies 51

[7] Oxforddictionaries.com, 'Pornography' (Oxford Dictionaries, n.d.) <http://www.oxforddictionaries.com/definition/english/pornography> accessed 10 January 2016

[8] B. Williams & A. Owen, 'Report of the committee on obscenity and film censorship' (1979) 7772 Stationery Office 8.2

[9] N. Strossen, *Defending Pornography: Free Speech, Sex, and the Fight for Women's Rights* (1st, NYU Press, 2000) 320

[10] I. O'Donnell & C. Miller, *Child Pornography; Crime, computers and society* (1st, Willan Publishing 2007) 259

[11] J. Lindgren, 'Defining pornography' (1993) 114 University of Pennsylvania Law Review 1153.

[12] S. S. M. Edwards, 'A safe haven for hardest core' (1997) 8 Ent. L.R. 137

[13] Oxforddictionaries.com, 'necrophilia' (Oxford Dictionaries, n.d.) <http://www.oxforddictionaries.com/definition/english/necrophilia?q=necrophilia> accessed 9 February 2014

recording of an actual murder"[14]. The diverse range of content, which can be considered pornographic is however subject to change, as attitudes surrounding vulgarity vary. This is coupled with changing levels of tolerance and acceptability in society, which has led to the introduction of regulations for certain forms of imagery[15].

In seeking sexual gratification, an individual does not have free reign to seek or produce material of any type, and many jurisdictions have sought to legislate on the types of material that are legally acceptable forms of pornography. Illegal forms of what will be referred to at this point as pornography for simplicity of argument can generally be categorised into two main types, child sex abuse imagery and extreme pornography, of which the former is the focus of this thesis. The major problem initiated by pornography, is that it has not only sexualised the abuse of adults but also that of children who are unable to consent to such acts[16]. Images depicting the sexual abuse of children are now widespread, due mainly to the Internet and digital devices[17]. This material has triggered significant public outrage, arguably considered in today's society as the worst form of material that can be characterised (albeit incorrectly) as pornographic, causing harm to both the child depicted and to society as a whole.

1.1 Addressing Terminology Used in this Thesis

To provide a starting point for discussions in this thesis, appropriate terminology in relation to this topic is considered. Wortley and Smallbone[18] refer to images that depict child sexual abuse as 'Internet Child Pornography' or ICP. Pritcher *et al*.[19] use the term child exploitation material. UK legislation prefers the terms Indecent Image of a Child. Akdeniz[20] utilises the term 'child pornography' stemming from its frequent use in foreign legislative documents, seen with the Council of Europe's Convention on Cyber Crime. There is no globally accepted

[14] Oxforddictionaries.com, 'snuff movie' (Oxford Dictionaries n.d.) <http://www.oxforddictionaries.com/definition/english/snuff-movie?q=snuff+movie> accessed 9 February 2014

[15] I. O'Donnell & C. Miller, *Child Pornography; Crime, computers and society* (1st, Willan Publishing 2007) 259

[16] C. A. MacKinnon, 'Pornography, civil rights, and speech' (1985) 20 *Harv. CR-CLL Rev*. 1

[17] Y. Akdeniz, *Internet Child Pornography and the Law: National and International Responses* (1st, Ashgate Publishing 2013) 326

[18] R. Wortley & S. Smallbone, *Internet Child Pornography: Causes, Investigation, and Prevention* (1st, ABC-CLIO 2012) 157

[19] J. Prichard, C. Spiranovic, P. Watters & C. Lueg, 'Young people, child pornography, and subcultural norms on the Internet.' (2013) 64 Journal of the American Society for Information Science and Technology 992

[20] Y. Akdeniz, *Internet Child Pornography and the Law: National and International Responses* (1st, Ashgate Publishing, 2013) 326

term for referencing child sex abuse imagery. However, there is a growing consensus that the inclusion of the word 'pornography' is objectionable when referring to this form of material[21].

It is suggested that through an inclusion of the term 'pornography' when referring to child sexual abuse images, the illegal material is being unacceptably glorified, providing support for, or condoning such acts[22]. Similarly, the term pornography may seek to lessen the seriousness of the offence or the harm suffered by the victim[23]. As a term, pornography generally denotes consensual, acceptable and legal acts of sexual activity and using it in relation to child images provides connotations that such abuse is also acceptable or tolerated[24]. The acts depicted in child sexual abuse images are neither consensual or lawful and therefore it is argued the their association with the term 'pornography' should cease. Quayle suggests that the term pornography implies consent, which cannot be given in cases involving children and therefore a move should be made to relinquish its use when associated with child abuse images[25]. This is despite many jurisdictions including Canada, Ireland and the US continually using it as a legal term in reference to this material.

The terminology of indecent images of children (IIoC) is used within legislation within England and Wales and merits brief discussion. Domestic legislation in England and Wales has opted to omit any reference to pornography in preference for the term indecent. By definition, the term indecent means 'not conforming with generally accepted standards of behaviour, especially in relation to sexual matters'[26]. It could be argued that even through the use of 'indecent', domestic legislation fails to recognise the actual harm, which is caused to the child, only referencing the act itself. In addition, by the very definition, 'indecent' simply implies the act is generally unacceptable. In reality the act of child sexual abuse is never acceptable and the term 'indecent' fails to underline the seriousness of the act.

---

[21] Y. Akdeniz, *Internet Child Pornography and the Law: National and International Responses* (1st, Ashgate Publishing, 2013) 11

[22] Y. Akdeniz, *Internet Child Pornography and the Law: National and International Responses* (1st, Ashgate Publishing, 2013) 11

[23] R. Wortley & Smallbone, S., *Internet Child Pornography: Causes, Investigation, and Prevention* (1st, ABC-CLIO, California 2012) 9

[24] E. Quayle 'The COPINE project' (2008) 5 Irish Probation Journal 65, 67

[25] E. Quayle 'The COPINE project' (2008) 5 Irish Probation Journal 65

[26] Oxforddictionaries.com, 'Indecent ' (Oxford Dictionaries n.d.) <http://www.oxforddictionaries.com/definition/english/indecent?q=indecent> accessed 15 March 2014

Despite legislation within England and Wales using the term indecent images of a child, it is argued that 'images depicting child sexual abuse' (IDCSA) is a preferable term for use in reference to such material and one which will be championed by this thesis with support from the Internet Watch Foundation (IWF) [27] and Interpol[28]. The inclusion of the words 'sexual abuse' ensures the gravity of the act is identified without connotations of glorifying or condoning it. The inclusion of the word abuse; defined as 'to treat with cruelty or violence, especially regularly or repeatedly[29]', limits the chance of misinterpretation regarding the condemnation of this material. Therefore IDCSA is seen as an acceptable term for conveying the severity of this material and will be used throughout the remainder of this thesis.

1.2 An Introduction to Child Sex Abuse Imagery and Societal Perceptions

Acts that constitute a crime change over time, geographical location and the development of public morals and values [30], with a similar transition visible within England and Wales. It was not until the 1970s that involvement with IDCSA was widely regarded as inexcusable and such material began to enter the public consciousness as media coverage increased[31]. Those connected with such material are now widely subject to significant stigmatisation, and, viewed as indefensible[32], signifying society's want for such offences to be punished by law and the need for legislation to prohibit IDCSA.

Individuals associated with these child sex abuse offences are often classified by society as paedophiles, despite the usage of the term to describe such persons being subject to scrutiny (a point of debate beyond the scope of this thesis). Paedophiles are defined as those who are sexually attracted to pre-pubescent children and/or material depicting such individuals[33] and are frequently considered "the bogeyman of our age"[34]. The word itself strikes fear and outrage into many members of society, sparking emotive reactions and

[27] Internet Watch Foundation, 'About Us' (IWF, n.d.) <https://www.iwf.org.uk/about-iwf> accessed 14 May 2015

[28] Interpol, 'Appropriate Terminology' (Interpol, n.d.) <http://www.interpol.int/Crime-areas/Crimes-against-children/Appropriate-terminology> accessed 2015 November 2

[29] Oxforddictionaries.com, 'Abuse' (Oxford Dictionaries n.d.) <http://www.oxforddictionaries.com/definition/english/abuse> accessed 12 September 2014

[30] J. Silverman & D. Wilson, *Innocence Betrayed Paedophilia, the Media and Society* (1st, Blackwell Publishing 2002) 2

[31] P. Jenkins, *Beyond Tolerance: Child Pornography on the Internet* (1st, NYU Press 2003)

[32] P. Jenkins, *Beyond Tolerance: Child Pornography on the Internet* (1st, NYU Press 2003) 4

[33] J. Silverman & D. Wilson, *Innocence Betrayed Paedophilia, the Media and Society* (1st, Blackwell Publishing 2002)

[34] J. Silverman & D. Wilson, *Innocence Betrayed Paedophilia, the Media and Society* (1st, Blackwell Publishing 2002) 1

public frenzy against those who are associated with the term. Child abuse offences have now reached such a heighten state of disgrace that even misinformed and propagandised information is enough to spark prejudicial public acts[35]. Silverman and Wilson[36] attribute the rise of public outrage against paedophilia and child offences to the abduction and murder of Sarah Payne in 2000[37] and the campaigns by the News of the World which followed in order to 'name and shame' convicted paedophiles. Similarly the difficulty of identifying, preventing and punishing those who are involved with IDCSA has increased society's anxiety[38]. Acts of public violence, community unrest and vigilantism against potential suspects are regularly witnessed, even in cases following negligent and erroneous media reports[39].

It is clear that society strongly opposes acts of child sex abuse and related activities, but a distinction is often made between contact offenders, recently brought into the public eye via the disgraced celebrities Jimmy Saville[40] and Iain Watkins[41], and non-contact offenders; those who only seek IDCSA. The latter form the focus of this thesis. Non-contact offenders are now largely dependent on technology in order access and acquire IDCSA and, a result, the Internet has now significantly increased the volume of IDCSA in circulation whilst allowing a wider audience access to it. The following section analyses the full extent to which technology has impacted upon IDCSA offences.

1.3 Availability of IDCSA: A Transition from Paper to Digital

Taylor suggested that in 1999, the scale of the issue posed by IDCSA had reached a stage where it was impossible to quantify the number of images in circulation[42] with the IWF recently reporting a 417% increase in reports of illegal imagery hosted online in 2015[43]. This is largely due to the development of the Internet, digital imagery and video files, which have

[35] J. Silverman & D. Wilson, *Innocence Betrayed Paedophilia, the Media and Society* (1st, Blackwell Publishing 2002) 1

[36] J. Silverman & D. Wilson, *Innocence Betrayed Paedophilia, the Media and Society* (1st, Blackwell Publishing 2002) 2

[37] Anon, 'Timeline: The Sarah Payne tragedy' *BBC News* (London, 12 December 2001) <http://news.bbc.co.uk/1/hi/england/1703534.stm> accessed 8 February 2014

[38] B. Ryder, 'The Harms of Child Pornography Law' (2002) 32 U. Brit. Colum. L. Rev. 101, 102

[39] Y. Jewkes & C. Andrews, *Internet Child Pornography: International Responses* in Willian (eds), *Crime Online* (1st, Willan Publishing 2007).

[40] N. Triggle, 'Jimmy Savile NHS abuse victims aged five to 75' *BBC News* (London, 26 June 2014) <http://www.bbc.co.uk/news/uk-28034427> accessed 1 September 2014

[41] Anon, 'Lostprophets' Ian Watkins sentenced to 35 years over child sex offences' *BBC News* (18 December 2013) <http://www.bbc.co.uk/news/uk-wales-25412675> accessed 1 September 2014

[42] M. Taylor, 'The nature and Dimension of Child Pornography on the Internet' Paper presented at the international conference 'Combating Child Pornography on the Internet' (1999)

[43] Internet watch foundation, 'IWF announce record reports of child sexual abuse online' (*Iwforguk*, 7 May 2016) <https://www.iwf.org.uk/about-iwf/news/post/444-iwf-announce-record-reports-of-child-sexual-abuse-online> accessed 7 May 2016

accentuated the volume of IDCSA that can be acquired by offenders. From one video, hundreds of still photographic images can be extracted and circulated[44]. In addition, technological developments have led to the creation of what can be termed as virtual child sex abuse imagery, consisting of images produced solely through sophisticated software, which do not originate from a living victim[45]. This has created a position where now, those who wish to engage with IDCSA no longer need to be involved in a physical act of child abuse or physically engage with another person to acquire the material.

The demand to obtain and view IDCSA is driven by the desire for sexual satisfaction achieved by viewing the material[46]. The actual extent of the issue posed by IDCSA is unknown and arguably likely to remain that way as paedophile networks actively seek to remain hidden and operate in unknown and obfuscated areas of the Internet[47]. Jewkes and Andrews note that it is not simply those who are perceived as the stereotypical 'grubby inadequate loners' who seek to obtain IDCSA, in fact the problem is wide spread across multiple cultures, religions and professions[48].

Technology has now allowed persons to source sexual gratification from digital images using computer systems as opposed to physical photographs, magazines or seeking out children to sexually abuse. Although links between viewing material depicting child sexual abuse and carrying out physical sexual abuse are not definitively established (see chapter 2 for further discussion), a demand to view such material is a driving force behind new acts of child abuse in order to create such imagery. The role that technology has had on IDCSA offences cannot be underestimated[49]. Specifically, the Internet has had a substantial impact on increasing the production and distribution this illegal material, whilst its perceived anonymity offers users the chance to exercise their sexual preference from within the confines of their home, potentially undetected[50]. The creation of the Internet can be seen as a milestone in the development of IDCSA offences despite remaining a relatively new invention. Although

[44] M. Taylor, 'The nature and Dimension of Child Pornography on the Internet' Paper presented at the international conference 'Combating Child Pornography on the Internet' (1999)
[45] J. Jauron, 'Paperless Pornography' (1994) 1 EDI L. Rev. 163, 166
[46] R. Wortley & S. Smallbone, *Internet Child Pornography: Causes, Investigation, and Prevention* (1st, ABC-CLIO 2012) 157
[47] Y. Akdeniz, *Internet Child Pornography and the Law: National and International Responses* (1st, Ashgate Publishing 2013) 326
[48] Y. Jewkes & C. Andrews, 'Internet Child Pornography: International Responses' in Willian (eds), *Crime Online* (1st, Willan Publishing, Devon 2007).
[49] G. Horsman, 'The challenges surrounding the regulation of anonymous communication provision in the United Kingdom.' (2016) 56 Computers & Security 151
[50] G. Horsman, 'The challenges surrounding the regulation of anonymous communication provision in the United Kingdom.' (2016) 56 Computers & Security 151

IDCSA is now thought to be predominantly hosted and distributed online, this has not always been the case. As a result, the following two sections will examine the impact that the Internet has had on IDCSA by considering the position before its creation and after.

1.3.1 Child Sex Abuse Imagery Before the Internet and Digital Technologies

Tate highlights that accounts of what is now considered in law as acts of child abuse, have been recognised throughout many historical archives[51]. Similarly, written records and stories depicting sexual acts with children still remain in circulation, including *Fanny Hill* and *Memoirs of a Woman of Pleasure*[52]. Not only were such acts recognised in forms of media, but also, cultural procedures frequently allowed this abuse to take place. In Greek civilisations records indicated children as young as 12 frequently engaged in sexual relationships with adults as old as 20[53]. Similar acts can be seen in Roman cultures where the average age of marriage for a female child was 14[54].

Prior to the year 2000 and the Internet's popularity, images depicting the sexual abuse of children existed in many tangible forms. Magazines such as 'Lollitots', 'Lolita', 'Piccolo', 'Rare Boys' and 'Tommy' were prevalent publications, along with various books depicting graphic scenes of child abuse[55]. In addition, numerous paedophile organisations had formed including 'The Rene Guyon Society', 'The North American Man/Boy Love Association', 'The Childhood Sensuality Circle', 'Paedophile Information Exchange' and 'The Howard Nichols Society'[56]. Also, what is termed as 'sex tourism' was emerging, often where the paedophile would visit deprived nations where laws governing child sexual abuse are limited in order to sexually abuse children and acquire IDCSA[57]. Yet without the resources for mass communication and organisation, which has now been provided by the Internet, paedophiles, as a group remained relatively isolated with limited methods to connect to one another[58]. In addition, without the use of devices capable of replicating, creating and

[51] T. Tate, *Child Pornography: An Investigation* (1st, Methuen 1990)
[52] W. M. Kendrick, *The Secret Museum: Pornography in Modern Culture* (1st, University of California Press 1987) 318
[53] R. Wortley & S. Smallbone, *Internet Child Pornography: Causes, Investigation, and Prevention* (1st, ABC-CLIO 2012) 157, 9
[54] ibid 9.
[55] S. T. Holmes & R. M. Holmes, *Sex Crimes Patterns and Behaviours* (1st, Sage Publications 2002) 291
[56] ibid 109.
[57] I. O'Donnell & C. Miller, *Child Pornography; Crime, computers and society* (1st, Willan Publishing 2007) 259
[58] E. Quayle & M. Taylor, 'Paedophiles, pornography and the Internet: Assessment issues' (2002) 32.7 British Journal of Social Work 863

distributing imagery within seconds, the production and dissemination of IDCSA was stunted, confined to those who were determined to actively seek them.

Yet the increasing affordability of digital technologies combined with access to the Internet is often viewed as a catalyst for growth in IDCSA offences.

1.3.2 The Impact of Increasing Digital Technology Usage and the Internet

The vast majority of prosecutions for child sex abuse imagery related offences now surround pictures that are found on digital storage media in computing equipment[59]. Often these images are acquired from on-line Internet sites hosting this material or acquired from other online sources. The Internet and computing devices have created a platform for likeminded persons to converse with one another, whilst allowing the individual to easily find and access them, and is arguably the driving force behind this offence. Academics have criticised the limited sanctions imposed on hosting material on the Internet, which has led to a range of sexualised content and now illegal imagery becoming available[60]. Sexualised content is now widespread online with "porn now one of the most frequent search terms used on Google"[61]. The existence of child sexual abuse imagery in society and the exponential growth of this content have been blamed on the commercialisation of the Internet[62]. O'Donnell and Miller highlight that in 1993, there were only fifty known websites, in comparison to the present day where due to the speed of growth, it is impossible to provide an accurate figure[63]. It wasn't until law enforcement launched 'Operation Ore' in 1999 to crack down on access to IDCSA on a pay-per-view website that websites hosting IDCSA gained public attention[64]. In fact, police manoeuvres such as 'Operation Ore' (an investigation in the Landslide Productions portal used to access images depicting child sexual abuse[65]) in the 1990s were considered rare, sparking limited public attention in comparison to the present day, where such operations remain heavily in the public's focus. During this period, it was acknowledged that experts investigating these offences were still significantly short of the

[59] K. Willmore, 'Protecting child victims' rights as vigorously as criminal defendants' when prosecuting possession or distribution of child pornography.' (2012) 87.3 Washington Law Review 887

[60] D. S. Thomas 'Cyberspace pornography: Problems with enforcement' (1997) 7.3 Internet Research 201

[61] HC Deb, 12th June 2013, vol 564, col 396

[62] I. O'Donnell & C. Miller, *Child Pornography; Crime, computers and society* (1st, Willan Publishing 2007) 259 and M. Johnson & K. M. Rogers, 'Too Far Down the Yellow Brick Road - Cyber-Hysteria and Virtual Porn' (2009) 4 J. Int'l Com. L. & Tech. 61, 61

[63] I. O'Donnell & C. Miller, *Child Pornography; Crime, computers and society* (1st, Willan Publishing 2007) 259

[64] J. Carr, *Child abuse, child pornography and the Internet* (1st, NCH 2003)

[65] A. A. Gillespie, 'Incitement to distribute indecent photographs of children revisited' (2011) 75.3 J. Crim. L. 168, 168

knowledge required to fully understand and appreciate the threats posed by this new technology[66]. Yet now, it is difficult to imagine a society without access to the Internet and its associated services, due to a new found dependence on this technology.

Statistics show that in 2015, 86% of households in the UK have Internet access, with 78% of UK adults accessing the Internet on a daily basis[67]. These figures also show an increase in the volume of children aged between six and seventeen who are now regular users of the Internet[68]. When combined with lowering device costs, the majority of UK households now own a personal computer[69] making sexualised imagery easily accessible via simple web-based searches. In addition, the popularity of mobile devices has notably increased and the introduction and growing popularity of the smartphone has now arguably made the availability of and access to pornographic content easier, with figures showing that 53% of all mobile phone owners use their device to access the Internet[70]. Further, better Internet connection speeds are also influencing the usage of the Internet as a medium to transfer IDCSA[71].

The Internet has provided a number of online facilities, which are abused by those who want to access and distribute IDCSA, whilst providing a platform for like-minded individuals to converse and seek support[72]. Newsgroups are a type of online forum where access can be restricted and only acquired via a distributed passkey. These provide a place where individuals can discuss and post information surrounding their common interest, providing an element of anonymity to the user[73] and often where the child sex abuse imagery

---

[66] Y. Akdeniz, *Internet Child Pornography and the Law: National and International Responses* (1st, Ashgate Publishing 2013) 326

[67] Office of National Statistics, 'Internet Access – Households and Individuals: 2015' (*ONS*, 6 August 2015) <http://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2015-08-06#household-internet-access> accessed 22 June 2016

[68] J. Davidson & P. Gottschalk, *Internet Child Abuse Current Research and Policy* (1st, Routledge 2011) 197

[69] Office of National Statistics*, Chapter 4 - Housing and Consumer Durables (General Lifestyle Survey Overview - a report on the 2011 General Lifestyle Survey)* (2013) 6

[70] Office of National Statistics, *Internet Access – Households and Individuals* (2013), 34 and J. Clough, 'Lawful Acts, Unlawful Images: The Problematic Definition of Child Pornography' (2012) 38 Monash U. L. Rev. 213

[71] G. Ivezaj, 'Child Pornography on the Internet: An Examination of the International Communities Proposed Solutions for a Global Problem' (1999) 8 Mich. St. U.-DCL J. Int'l L. 819, 823

[72] R. Cohen-Almagor, 'Online Child Sex Offenders: Challenges and Counter-Measures.' (2013) 52.2 The Howard Journal of Criminal Justice 190

[73] I. O'Donnell & C. Miller, *Child Pornography; Crime, computers and society* (1st, Willan Publishing 2007) 259

themselves operate as a form of online currency[74]. Bulletin Board Systems (BBS) are similar to newsgroups but provide a real time system where text and images can be frequently displayed and updated[75]. BBS can be used to provide instantaneous updates regarding the location of IDCSA and the ways in which it can be accessed. Ivezaj states in 1999, BBS accounted for over 20% of all child sex abuse imagery on the Internet[76]. With the use of these functions exacerbating the volume of IDCSA in circulation comes the needs to regulate such Internet services.

Calls have been made for Internet service providers to take more of an active role in the policing of IDCSA to stem the availability, and, to have more responsibility for preventing access to it[77]. The introduction of online mandatory filters requiring 'op-in's' from customers in order to access certain categories of material could soon be implemented by all of the major ISPs in the UK[78]. Attempts have also been made, in conjunction with Association For Payment Clearing Services in the UK to monitor and trace individuals who use their credit card details to purchase or access online IDCSA[79.] Typically when IDCSA is found on a UK based server and reported its presence will be removed within hours, making it inaccessible to other users[80]. However, such response times are not often witnessed when material is hosted abroad leading to the availability of IDCSA being prolonged, in some cases, reported websites remained in action over 12 months after initial reports were made[81]. As well as the ability to report illicit websites, advances in the reliability of website blocking technology (seen since 2006) have made it easier to restrict access to IDCSA[82]. As part of the effort

[74] E. Quayle & M. Taylor, 'Paedophiles, pornography and the Internet: Assessment issues.' (2002) 32.7 British Journal of Social Work 863

[75] E. Quayle & M. Taylor, 'Paedophiles, pornography and the Internet: Assessment issues.' (2002) 32.7 British Journal of Social Work 863

[76] G. Ivezaj, 'Child Pornography on the Internet: An Examination of the International Communities Proposed Solutions for a Global Problem' (1999) 8 Mich. St. U.-DCL J. Int'l L. 819, 823

[77] Culture, Media and Sport Committee, Online Safety (HC 2013, 125-222) available at <http://www.publications.parliament.uk/pa/cm201314/cmselect/cmcumeds/729/729.pdf> accessed 16 January 2016

[78] Culture, Media and Sport Committee, Online Safety (HC 2013, 125-222) available at <http://www.publications.parliament.uk/pa/cm201314/cmselect/cmcumeds/729/729.pdf> accessed 16 January 2016

[79] J. Davidson, J. Grove-Hills, A. Bifulco, P. Gottschalk, V. Caretti, T. Pham, & S. Webster, 'Online abuse: literature review and policy context' (2011) European Online Grooming Project <http://www.scotcen.org.uk/media/22523/european-online-grooming-projectliteraturereview.pdf> accessed 14 June 2016

[80] J. Carr & Z. Hilton, 'Combatting Child Abuse Images on the Internet' in J. Davidson & P. Gottschalk (eds), *Internet Child Abuse Current Research and Policy* (1st, Routledge 2011)

[81] J. Carr & Z. Hilton, 'Combatting Child Abuse Images on the Internet' in J. Davidson & P. Gottschalk (eds), *Internet Child Abuse Current Research and Policy* (1st, Routledge 2011)

[82] T. J. McIntyre, 'Blocking child pornography on the Internet: European Union developments' (2010) 24.3 International Review of Law, Computers & Technology 209

made by the IWF, the search engines Google and Microsoft's Bing now block results for 100,000 search terms in 158 different languages[83]. The acknowledgement of a need to block online content has also been discussed in the European Parliament. Directive 2011/92/EU on 'combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA', article 25 states that member states should take prompt action to remove illegally hosted material and may implement blocking techniques to restrict access to online content. Yet despite moves towards regulating IDCSA, it still remains prominent online.

Even with regulating statutes, material that remains undiscovered is difficult to control. IDCSA may only be hosted for a limited amount of time, long enough to inform offenders so that they can quickly download before the host site is shut down in order to evade regulating authorities[84]. Around the turn of the millennium *Reka et al*.[85] noted that a seemingly exponential growth of the Internet's infrastructure meant that websites were being created which were unknown to many service providers. This point is placed in context as Reka *et al*.[86] highlight that search engines at this point in time had only indexed an estimated 38% of the Internet, where now it likely remains far less due to it's exponential growth. Further, consideration must also now be given to the 'deep web', a portion of the Internet, which cannot be found using traditional search engines. The deep web offers access to numerous hidden services, which are often cited to have links to IDCSA distribution[87], where recent studies have demonstrated the ease and availability of this material on the platform[88]. With these developments, Section 1.4 considers the present situation surrounding the regulation of IDCSA.

1.4 The Current Situation with IDCSA

There is no doubt that those involved with IDCSA are committing one of the gravest offences in English law. However despite global condemnation, IDCSA offences are still prominent. Statistics show that offences surrounding IDCSA were the second most encountered digital

[83] D McGurran, 'Cambridge's Internet Watch Foundation leads child abuse clean up' *BBC News* (Norfolk, 20 November 2013) <http://www.bbc.co.uk/news/25005541> accessed 15 March 2014
[84] I. O'Donnell & C. Miller, *Child Pornography; Crime, computers and society* (1st, Willan Publishing 2007) 259
[85] A. Réka, H. Jeong & A. Barabási, 'Internet: Diameter of the world-wide web' (1999) 401 Nature 130, 130
[86] A. Réka, H. Jeong & A. Barabási, 'Internet: Diameter of the world-wide web' (1999) 401 Nature 130, 130
[87] A. Phelps & A. Watt, 'I shop online–recreationally! Internet anonymity and Silk Road enabling drug use in Australia.' (2014) 11.4 Digital Investigation 261
[88] D. Moore & T. Rid, 'Cryptopolitik and the Darknet.' (2016) 58.1 Survival 7

offence by police in Europe and America in 2013[89]. In turn, it has been identified that in 2008, around 80% of cases investigated by digital forensic organisations surround this offence type[90] with this trend showing no sign of decline. Figures provided by the Child Exploitation and Online Protection Centre (CEOP) "show that only one in every 15 people caught viewing child pornography on the Internet is arrested" [91]. Technology has transformed the way IDCSA is produced, distributed and possessed and now undoubtedly plays a significant role in the prominence of IDCSA offences.

CEOP [92] is an organisation committed to eliminating child sexual abuse and gathers intelligence on offenders and their behaviour. In 2012-13 CEOP intervened and protected 790 children from sexual abuse, distributed 2866 intelligence reports of overseas child abuse and arrested 192 suspects for child exploitation[93]. However this figure is almost certainly far less than the actual number of child victims which likely remain unknown to law enforcement and offenders in circulation. Many forms IDCSA depict acts of sexual abuse with a living child, where, in many cases it is impossible to determine who the child is or whether the abuse is continuing. Interpol's[94] International Child Sexual Exploitation image database (ICSEDB) provides a central repository for IDCSA for the purposes of victim identification, a facility utilised by 40 countries. By 2013, its use had led to the identification of almost 3900 victims and led to the prosecution and identification of over 1900 offenders[95]. Yet despite the historic comments of Taylor who notes that many child abuse victims remain unknown; and it is likely that the number of victims is increasing due to the continuous demand for IDCSA, it is probable that this situation is accurate today[96]. This is arguably due in part to online communities of individuals engaging in child abuse.

[89] United Nations Office on Drugs and Crime 'Comprehensive Study on Cyber Crime' (2013) pg.26
[90] S. Peisert, M. Bishop & K. Marzullo, 'Computer Forensics In Forensis.' (2008) Proceedings of the Third International IEEE Workshop on Systematic Approaches to Digital Forensic Engineering (IEEESADFE) 102
[91] HC Deb, 12th June 2013, vol 564, col 397
[92] Anon, 'About the CEOP Centre' *CEOP* (Child Exploitation and Online Protection Centre 2013) <http://ceop.police.uk/About-Us/> accessed 24 August 2013
[93] CEOP, Annual Review 2012-2013 & Centre Plan (2013), pg.7
[94] Anon 'Crimes Against Children' COM/FS/2013-10/THB-03 (Interpol 2013) <www.interpol.int/content/download/19248/170122/version/15/file/Factsheets_EN_oct2013_THB03%20web.pdf> accessed 15 June 2014
[95] Anon 'Crimes Against Children' COM/FS/2013-10/THB-03 (Interpol 2013) <www.interpol.int/content/download/19248/170122/version/15/file/Factsheets_EN_oct2013_THB03%20web.pdf> accessed 15 June 2014
[96] M. Taylor 'The nature and Dimension of Child Pornography on the Internet.' Paper presented at the international conference 'Combating Child Pornography on the Internet' (1999)

1.4.1 Thriving online Networks

Quayle and Taylor[97] highlight a key issue surrounding modern day concerns with IDCSA offenders. Before the dominance of digital media and mass communication, the production and dissemination of this material was stunted. This can be perceived both positively and negatively. The inability to produce, distribute and communicate with likeminded individuals reading IDCSA may have restricted this illegal material to small pockets of confined individuals, protecting society from the potential for corruption. Without knowledge of it, there can be no curiosity to seek it out and view it. Conversely, limited access to IDCSA may have led to increased physical forms of abuse as paedophiles seek to act out their fantasies. Regardless of these issues, volumes of IDCSA are now significantly larger where thousands of pictures can be created in seconds across vast thriving online communities.

The problems posed by the Internet stem from what Akdeniz[98] describes as its global, borderless and decentralised nature allowing an unlimited number of people to communicate across multiple jurisdictions. International borders are seemingly non-existent in the online community[99]. The Internet is a worldwide network of computers, which communicate and share information with one another[100]. It allows users to go anywhere and communicate with anyone, often with limited restrictions in place[101]. Jenkins provides that "the Internet is neither a place or a thing, but a construct of millions of individual servers which we happen to describe through a visual metaphor of the Internet or web"[102]. The Internet also offers a low cost and low risk method of acquiring and distributing IDCSA in comparison to previously implemented methods such as via post or physical in-person transactions where material is traded [103]. Due to the geographical expansion and layout of the Internet, differing legislation and jurisdictions, which take divergent standpoints on topics such as the age of consent and adulthood, mean a global approach to policing IDCSA

[97] E. Quayle & M. Taylor, 'Paedophiles, pornography and the Internet: Assessment issues.' (2002) 32.7 British Journal of Social Work 863

[98] Y. Akdeniz, *Internet Child Pornography and the Law: National and International Responses* (1st, Ashgate Publishing 2013) 326

[99] J. Kortlander, 'Is filtering the new silver bullet in the fight against child pornography on the internet? A legal study into the experiences of Australia and Germany' (2011) 17.7 Computer and Telecommunications Law Review 199, 199

[100] D. Crystal, *Language and the Internet* (1st, Cambridge University Press, 2001)

[101] E. Quayle & M. Taylor, 'Paedophiles, pornography and the Internet: Assessment issues' (2002) 32.7 British Journal of Social Work 863

[102] P. Jenkins, *Beyond Tolerance: Child Pornography on the Internet* (1st, NYU Press 2003) 260, 5

[103] L. M. Jones, 'Regulating Child Pornography on the Internet - The Implications of Article 34 of the United Nations Convention on the Rights of the Child' (1998) 6 Int'l J. Child. Rts. 55, 57

is almost impossible[104]. This has led to Russia, eastern European, and Asian countries being frequently identified as sources of child sexual abuse imagery[105]. Illegal pornography is often hosted in countries with poor legal systems, which are unlikely to co-operate with the UK in absence of a prior agreement[106]. This means that in many cases, it is impossible to police offences as both the suspects and material may be subject to different legislative powers and restraints.

It is estimated that 54% of IDCSA is hosted in North America; 37% is hosted across Europe and Russia; 1% in Asia and less in South America highlighting the global problem posed[107]. In 2013, the IWF removed 10,000 websites, of which 35 were hosted in the UK[108]. Material hosted in foreign territories remains a major concern and outside of the control of the UK's jurisdiction. In cases of material reported which is hosted outside of the UK, IWF will inform the International Association of Internet Hotlines (INHOPE) organisation[109]. INHOPE are a collaborative network across 43 countries around the world dedicated to removing online child abuse material[110]. Statistics from 2012 show that INHOPE dealt with over one million reports of illegal material, 80% of which came from either the US, Canada or EU member states[111]. Although the IWF have made significant inroads into removing access to IDCSA, the availability of material hosted in foreign jurisdictions still poses an issue. The Labour MP Helen Goodman has expressed the following concerns surrounding the task faced by IWF.

> The problem with that is that the Internet Watch Foundation is hugely strapped for cash and unable to deal with all the alerts it receives. It is worried, because a survey that it undertook has suggested that, although 1.5 million people have seen child abuse images, only 40,000 reports have been made to the organisation[112].

Placing some form of restriction on access to IDCSA is key as Jenkins argues that it is impossible to eliminate this material from within the realms of the Internet and may even be

---

[104] J. Davidson, M. Lorenz, E. Martellozzo, & J. Grove-Hills, *Evaluation of CEOP Think U Know Internet Safety Programme and Exploration of Young People's Internet Safety Knowledge* (1st, 2010)
[105] J. Carr, *Child abuse, child pornography and the Internet* (London, NCH 2003)
[106] P. Sommer, 'Evidence in Internet paedophilia cases' (2002) 8.7 C.T.L.R. 176
[107] HC Deb, 12th June 2013, vol 564, col 383
[108] D McGurran, 'Cambridge's Internet Watch Foundation leads child abuse clean up' *BBC News* (Norfolk, 20 November 2013) <http://www.bbc.co.uk/news/25005541> accessed 15 March 2014
[109] I. Walden, 'Safeguards in the ether' (2010) European Lawyer 53, 53
[110] Anon, 'At A Glance' *INHOPE* (INHOPE n.d.) <http://www.inhope.org/gns/who-we-are/at-a-glance.aspx> accessed 19 March 2014
[111] INHOPE, 'Annual Report 2012' (2012) 13
[112] HC Deb, 4th July 2013, vol 565, col 1142

beyond the possibility of being suitably policed[113]. This view is also shared by other academics[114]. The Internet is not simply a medium for the exchange of graphical depictions of child sexual abuse. Websites have been noted to contain literary portrayals of indecent sexual acts with children providing a stimulus for offenders to seek physical contact with children[115].

Jenkins argues that although the acquisition of non-electrical forms of child sexual abuse imagery is now extremely difficult, the same is not true for material found on the Internet[116]. Individuals no longer need to seek out or physically visit contacts that are involved in this form of abuse in order to purchase material; the Internet provided a convenient and seemingly anonymous method of fuelling those who can already be termed as a having a fascination with it[117]. This has caused the Internet to generate a relatively new, unknown and under researched type of sex offender, which Webb[118] argues, differs from the contact sex offender where more research has been carried out (albeit still limited). In addition, where as those seeking to acquire physical images or magazines (in the traditional form of the offence) may be easier to track and monitor, the Internet has assisted in the generation of thousands of offenders who remain unknown and anonymous to law enforcement agencies, accessing child sex abuse imagery from the comfort of their home.

The Internet also poses the unique issue of causing the user to become disinhibited and more likely to access material, which they would not normally seek out. It provides an "unprecedented degree of inquisitiveness, and the danger is that curiosity hardens into deviance" as inhibitions are lost [119]. Similarly it offers a sense of protection to the user as they may feel that they are not physically identifiable while carrying out their online actions due to a lack of physicality. As a result, the Internet provides the environment for which a curiosity surrounding IDCSA can flourish[120]. Individuals can seek out material based on their own interests and desires as well as seek communication with self-justifying online

[113] P. Jenkins, *Beyond Tolerance: Child Pornography on the Internet* (1st, NYU Press 2003) 260
[114] Y. Akdeniz, *Internet Child Pornography and the Law: National and International Responses* (1st, Ashgate Publishing 2013) 326
[115] L. M. Jones, 'Regulating Child Pornography on the Internet - The Implications of Article 34 of the United Nations Convention on the Rights of the Child' (1998) 6 Int'l J. Child. Rts. 55, 57
[116] P. Jenkins, *Beyond Tolerance: Child Pornography on the Internet* (1st, NYU Press 2003) 5
[117] E. R. Diez, 'One Click, You're Guilty: A Troubling Precedent for Internet Child Pornography and the Fourth Amendment' (2006) 55 Cath. U. L. Rev. 759
[118] L. Webb, J. Craissati, & S. Keen, 'Characteristics of Internet child pornography offenders: A comparison with child molesters.' (2007) 19.4 Sexual abuse: a journal of research and treatment 449
[119] I. O'Donnell & C. Miller, *Child Pornography; Crime, computers and society* (1st, Willan Publishing 2007) 55
[120] M. Taylor & Quayle E., *Child pornography: an Internet crime. (*1st, Brunner-Routledge 2003)

communities interested in the illegal material[121]. In addition, anonymous Internet browsing protocols such as Tor onion routing (an Internet protocol for obfuscating communications across the Internet, effectively making them untraceable) provide the user with anonymity when accessing and sharing illegal material online[122] with Barratt *et al.* stating that the popularity of such tools and techniques has recently increased[123]. Tor currently provides unbreakable anonymity for the user, making it difficult for law enforcement to identify those accessing illegal content online along with a concealed directory of websites hosting IDCSA [124]. This ultimately makes the identification of suspects and prevention the distribution and access to online illegal pornography almost impossible[125].

When Internet access is coupled with the affordability of digital devices, there remains a greater potentially for a larger number of potential offenders to interact with IDCSA online, as discussed below.

1.4.2 Digital Devices and a Focus on Possession

Although the Internet has provided a means of disseminating illegal material, a founding issue (both in terms for development of IDCSA offences, and for discussions in this thesis) surrounds the transition from physical (photos etc.) to intangible (digital) forms of IDCSA. Computing technology allows individuals to store, create and access millions of intangible digital files almost instantaneously and provides the first issue for the regulation of possession of IDCSA. When combined with advances in camera and video-recording technologies, digital technology has allowed individuals the ability to amass and house vast archives of IDCSA with relative ease in comparison to achieving the same goal using tangible forms (paper, VHS etc.) of IDCSA.

A second concern is posed by the volatility of digital data. Unlike books and magazines, digital images and videos can be created and deleted in seconds. The consequence being, that individual's can become possessors of digital IDCSA in breach of English law within

[121] T. Krone, 'A typology of online child pornography offending.' (2004) Australian Institute of Criminology

[122] R. Dingledine, N. Mathewson & P. Syverson, 'Tor: The second-generation onion router' (2004) Naval Research Lab Washington DC 1, 1

[123] M. J. Barratt, S. Lenton & M. Allen, 'Internet content regulation, public drug websites and the growth in hidden Internet services.' (2013) 20.3 Drugs: education, prevention and policy 195

[124] R. Cohen-Almagor, 'Online Child Sex Offenders: Challenges and Counter-Measures.' (2013) 52.2 The Howard Journal of Criminal Justice 190

[125] M. Ward, 'Do dark networks aid cyberthieves and abusers?' BBC News Technology (20 June 2013) <http://www.bbc.co.uk/news/technology-22754061> accessed 19 January 2014

seconds, from the comfort of their own home, and within a similarly short timeframe, also part possession with IDCSA, where often there is limited evidence of these acts.

The third problem surrounds the complexity of computing systems; with many individuals not fully understand the consequences of their actions and digital footprint whilst using these devices. This can potentially result in breaches of illegal imagery laws and provides difficulties for law enforcement when trying to establish an accurate chain of events on a computer system for the purposes of establishing culpability. In comparison, establishing whether an individual is in possession of a tangible IDCSA can be established using traditional possession concepts (discussed in Chapter 4).

The aforementioned problems areas now mean the possessor of IDCSA (where digital imagery is involved) has now fundamentally changed, posing a new challenge to law enforcement both in terms of detection and regulation. In turn, the combination of computing devices and the Internet has now paved the way for greater number of individuals to potentially possess illegal imagery. The number of offenders engaging in these acts has arguably caused regulatory issues due to limited resources available to law enforcement for effective regulation.

It is estimated that approximately fifty thousand individuals within the UK are involved in the acquisition and distribution of IDCSA [126]. Statistics indicate that the number of individuals prosecuted for their involvement with IDCSA is growing[127]; yet it is arguable that the battle to control IDCSA is still being lost. An unforeseen risk, which has now developed partially due to the popularity of social media, is self-generated IDCSA (SGIDCSA, sexualised images taken by children and posted online)[128] allowing suspects to passively browse and acquire images and material voluntarily placed within the Internets domain. The true scale of the problem posed by IDCSA is stated by Johnson and Rogers who suggest that now, due to digital technologies, it will always be accessible to those who actively seek to obtain it,

[126] CEOP, 'Threat Assessment of Child Sexual Exploitation and Abuse' (2013) 8 < https://ceop.police.uk/Documents/ceopdocs/CEOP_TACSEA2013_240613%20FINAL.pdf > accessed 6 December 2015

[127] A. Lukas, 'Exploring the Extent to Which the Utilization of Technology Has Facilitated the Increased Possession of Online Child Pornography over Time.' (Masters of Science in Criminal Justice thesis, Kennesaw State University 2013)

[128] CEOP, 'Threat Assessment of Child Sexual Exploitation and Abuse' (2013) 11 < https://ceop.police.uk/Documents/ceopdocs/CEOP_TACSEA2013_240613%20FINAL.pdf > accessed 6 December 2015

however, detecting and prosecuting these individuals is difficult due to limited resources[129]. Helen Goodman, Labour MP echoed these views, highlighting the following current regulatory difficulties.

> … 60,000 people in this country are downloading child abuse images, yet its resources are so limited that it was able to secure only 1,570 convictions last year[130].

IDCSA depict children below the age of 18, and although those in possession of IDCSA may not have been directly involved in the original act and have acquired the online, those seeking to possess this material are arguably driving the production of it. This ultimately prompts more acts of child abuse to be carried out in order to cope with demand for this imagery. Further, trends in the last three years show the severity of depicted IDCSA to be increasing, with a greater quantity of images including both adults and children[131]. Those depicted are subject to considerable harm both mentally and physically, and, in turn, failure to condemn this behaviour may encourage further child abuse as more forms of media are produced[132.] Discussions surrounding harm to the child are expanded upon in Chapter 2.

One of the key issues surrounding IDCSA is the influence of technology on the offender. The possessor of IDCSA is now distinct to the possessor pre-Internet. Prior to the millennium the majority of offenders had previous child abuse convictions, however post 2006, many offenders are reported to have no previous criminal convictions of any sort[133]. This could suggest that the ease of access to this form of imagery is encouraging those who are curious about this illegal content to actively seek it out. The underlying problem stems from the perceived security of anonymity that the Internet provides is encouraging offending behaviour. These forms of "emerging technologies blur the line between conscience, expression and action in ways that cry out for an understanding of the harms of child pornography encompassing not just the extremely concerning physical harm to individual

[129] M. Johnson & K. M. Rogers, 'Too Far Down the Yellow Brick Road - Cyber-Hysteria and Virtual Porn' (2009) 4 J. Int'l Com. L. & Tech. 67

[130] HC Deb, 4th July 2013, vol 565, col 1142

[131] CEOP, 'Threat Assessment of Child Sexual Exploitation and Abuse' (2013) 8 < https://ceop.police.uk/Documents/ceopdocs/CEOP_TACSEA2013_240613%20FINAL.pdf > accessed 6 December 2015

[132] HL Deb 04 October 2000 vol 616 cc1564-89 and M. H. Silbert, 'On Effects on Juveniles of Being Used for Pornography and Prostitution' (1989), in D. Zillman and C. Bryant, *Pornography: Research Advances and Policy Considerations, (*Hillside, NJ: Lawrence Erlbaum)

[133] J. J. Exum, 'Making the Punishment Fit the (Computer) Crime: Rebooting Notions of Possession for the Federal Sentencing of Child Pornography Offenses.' (2009) 16 Rich. JL & Tech. 16 1, 32

children, but also broader social harms to children's collective dignity and equality rights"[134]. Barnardo's sexual exploitation services witnessed a 22% increase in the number of sexually exploited children in 2011-12 of which the majority of cases were linked to the use of the Internet [135].

There is no doubt that the possessor plays a pivotal role in the illegal imagery sphere, however, despite the act of possession of IDCSA being illegal within the UK, this thesis questions whether this legislation is still effective.

1.5 Is the Current Law effective?

It is arguable that since the advent of the Internet, there are now a greater number of potential possessors of IDCSA than ever before. However, given the transition from a predominantly paper-based market for IDCSA, to forms of digital media as noted above, the problems encountered within this area of law have now fundamentally changed. Therefore, this thesis will explore whether the current law on the possession of IDCSA is ineffective due to developments in technology and digital imagery. To provide a summary, the following four points of contention will be considered.

First, the offences of creating, distributing and publication were introduced in 1978 with the Protection of Children Act. It was not until some ten years later with the Criminal Justice Act 1988, that a possession offence was drafted into English law. Although amendments to these offences have occurred (e.g. recognition of digital files as a photograph and indecent drawings and tracings) the core number of IDCSA offences has not been expanded upon beyond those noted above. The key issue surrounding this area of law remains that legislation for policing access to, and, possession of IDCSA is arguably slow to respond to technological advances, which provide new ways to carry out the offences relating to IDCSA.

Second, at the time of production, the Criminal Justice Act 1988 was designed to combat IDCSA in forms of media prevalent at that time, such as magazines and videotapes. These items maintained a physical presence, which could be easily monitored by law enforcement. The replication of these forms of media is cumbersome and the quality is low. Further, distribution and acquisition of this material had to take place via a physical transaction between parties, increasing the risk of being caught and arguably deterring individuals. Yet,

[134] J. Bailey, 'Confronting Collective Harm: Technology's Transformative Impact on Child Pornography' (2007) 56 U.N.B.L.J. 65, 67

[135] HC Deb, 12th June 2013, vol 564, col 399

now technology has far surpassed the original thoughts, which drove the production of this legislation.

Third, the concept of possession of digital data is not straightforward and IDCSA now exists predominantly in an intangible digital form, which can be cloned and distributed thousands of times within seconds. A somewhat traditional application of the concept of possession involves the need to establish knowledge of, along with custody and control over a chattel before one can truly possess it. This application of a possession test has been confirmed in the leading case of *Porter*[136] regarding possession of IDCSA on a computing system. However the test itself is far from simple, requiring a subjective analysis of the offender's computing skills, an arguably impossible task, which could lead to unreliable results. The possession test also incurs difficulties when applied to deleted files and images found within the Internet cache on a computing system. The test appears to overlook the intricacies of computing operating systems, along with data that may be available via digital forensic investigation to support a prosecution. This has lead to an uncomfortable overlap between possession and the more severe offence of 'making' due to the case of *Smith and Jayson*[137], which has received academic criticism from Akdeniz[138].

Fourth, the legislation was never drafted with the commercialisation of the Internet in mind, leading to piecemeal developments, through case law. Online streaming protocols and anonymity services such as In-private browsing now allow individuals to access IDCSA online without 'possessing' the images, when applying current possession definitions. The issue here is that the individual who does this is technically 'accessing' material, not possessing, creating or making it. Yet, current legislation does not recognise the act of accessing. This gap in existing legislation is allowing individuals to view IDCSA whilst evading current defined law.

This thesis analyses these areas of concern, with the complete thesis structure noted below.

1.6 Thesis Structure

This thesis explores the scope of current IDCSA laws in England and Wales, with a focus on the offence of possession of IDCSA. The thesis is structured as follows:

[136] *Porter* [2006] EWCA Crim 560; [2006] 2 Cr. App. R. 25
[137] *R. v Smith (Graham Westgarth)* [2003] 1 Cr. App. R. 13 at 33
[138] Y. Akdeniz, 'Case report: Court of Appeal clarifies the law on downloading pornography from the Web.' (2002) 18.6 Computer Law & Security Review 433

Chapter 2 provides a discussion of the harms caused by IDCSA to society and the child whilst discussing the potential escalation of involvement of the offender in these offences. The aim of this chapter is to provide the reader with the underpinning knowledge as to why England and Wales regulate the possession of this material. The reader will also understand what constitutes IDCSA and the difficulties surrounding defining such material. The justifications for regulating IDCSA are presented and the different types of offender are discussed (creator, distributor, solicitor, possessor, viewer). The chapter will finally focus analysis on the 'possessor' and their impact on to continued circulation of IDCSA providing an understanding of the role of the possessor in relation to IDCSA, providing a platform from which current legislation can be analysed.

Chapter 3 examines the chronological development of the law surrounding IDCSA, commencing with the Obscene Publications Acts. Additional amendments to legislation such as the recognition of digital files as pictures and indecent drawings are included with available defences to IDCSA related offences presented. At the close of the chapter, the legal intricacies of IDCSA law and current day precedents will be presented, providing a background to this area and allowing for a focused analysis in Chapter 4 surrounding the offence of possession.

Chapter 4 presents an analysis of the general concept of possession and the offence of possession of IDCSA in English law. The aim of the chapter is to provide an in-depth understanding of possession law both in relation to IDCSA and other legal areas. The concept of possession is first analysed in terms of tangible and in-tangible data as well as a discussion of how possession applies in other offence types. Analysis of possession of IDCSA is provided, with the leading case of *Porter*[139] examined along with the test of possession for IDCSA, used in cases of possession of digital IDCSA. At the close of this chapter, the current application of laws in relation to possession of IDCSA will be identified.

Chapter 5 provides the reader with an analysis of the application of the possession test for IDCSA on computer systems and the intricacies of digital evidence. Discussions focus on deleted files and the Internet cache, two contentious topics in this area of law, whilst highlighting the use of digital forensic evidence in proving possession. The offence of possession and the data obfuscation technique of encryption are discussed in conjunction

[139] *Porter* [2006] 2 Cr. App. R. 25

with the Regulation of Investigatory Powers Act 2000. Finally the overlap between the offence of possession and that of 'making' is also scrutinised.

Chapter 6 concludes the thesis by providing some thoughts on legislative reforms surrounding possession of IDCSA, including the introduction of a new test for possession and a need for expanding the current range of offences to include that of 'accessing' IDCSA. Finally, conclusions are drawn regarding future legal developments in this area.

Chapter 2

The Harm Caused by IDCSA

2 Introduction

The focus of Chapter 2 is on the harm caused by IDCSA. It provides a discussion surrounding problems with defining an IDCSA, where both domestic and international positions are considered. It will then examine the harm caused by IDCSA, focusing on both the child and to society, with justifications for regulating the possession, distribution and creation of this material presented. The chapter then provides an analysis of the types of offender associated with IDCSA before focusing on the 'possessor' and their impact on the production and dissemination of illegal imagery. Counter arguments against the regulation of possession of IDCSA are briefly presented, before finally, conclusions are drawn.

2.1 What is an Image Depicting Child Sexual Abuse?

Within England and Wales there is no definition of an IDCSA provided by statute. In fact, of the 184 countries that are members of Interpol, only 94 had directly addressed the issue of IDCSA in their domestic legislation by the year 2008[140]. Jones[141] stated that in 1998 there was no one globally accepted definition of child sexual abuse images, the absence of which was preventing the control and research of such material. Arguably this position remains[142], where even in legislation in England and Wales, the PCA78 and CJA88 omit to define what they term as an indecent image of a child. When considering this issue of producing a definition of IDCSA, Gillespie states there are three problematic aspects: 'the age of the subject (what is a child), the nature of the material (what is being represented) and the type of material (what form does it take)' [143]. Determining whether an image of a child is illegal can depend on a number of factors such as the child's pose and picture context along with

[140] E. Quayle, 'The COPINE project.' (2008) 5 Irish Probation Journal 65

[141] L. M. Jones, 'Regulating Child Pornography on the Internet - The Implications of Article 34 of the United Nations Convention on the Rights of the Child' (1998) 6 Int'l J. Child. Rts. 55, 57

[142] J. Houtepen, J. J. Sijtsema & S. Bogaerts, 'From child pornography offending to child sexual abuse: A review of child pornography offender characteristics and risks for cross-over.' (2014) 19.5 Aggression and violent behavior 466

[143] A. A. Gillespie, 'Defining Child Pornography: Challenges for the Law' (2010) 22 Child & Fam. L. Q. 200, 201

societal moral and cultural beliefs[144]. England and Wales can look to the following definitions attempted by international legislation, such as that provided by the Council of Europe's Convention on Cyber Crime 2001 under Article 9:

> For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:
>
> a) A minor engaged in sexually explicit conduct;
> b) A person appearing to be a minor engaged in sexually explicit conduct;
> c) Realistic images representing a minor engaged in sexually explicit conduct.

In addition the European Union's Framework Decision combating the sexual exploitation of children and child pornography [145] provides the following under Article 1.

> a) "child" shall mean any person below the age of 18 years;
>
> b) "child pornography" shall mean pornographic material that visually depicts or represents:
>
> (i) a real child involved or engaged in sexually explicit conduct, including lascivious exhibition of the genitals or the pubic area of a child; or
> (ii) a real person appearing to be a child involved or engaged in the conduct mentioned in (i); or
> (iii) realistic images of a non-existent child involved or engaged in the conduct mentioned in (i);

Finally Article 2(c) of the 'Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography' provides[146].

> 2(c) Child pornography means 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.

All three definitions prefer the somewhat controversial phrase of 'child pornography' (which has already been addressed in Chapter 1) and place emphasis on the term 'sexually explicit'

[144] J. Houtepen, J. J. Sijtsema & S. Bogaerts, 'From child pornography offending to child sexual abuse: A review of child pornography offender characteristics and risks for cross-over.' (2014) 19.5 Aggression and violent behavior 466

[145] Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography

[146] Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, G.A. Res. 54/263, Annex II, 54 U.N. GAOR Supp. (No. 49) at 6, U.N. Doc. A/54/49, Vol. III (2000), entered into force January 18, 2002.

or ‘explicit sexual activity’ as the threshold for determining whether an image is of a pornographic nature. However, as with the issues posed by defining what constitutes ‘pornography’, similar issues here and the term ‘sexually explicit’ may not sufficiently catch all forms of IDCSA. To elaborate on this issue, Holmes and Holmes propose a definition focusing on images which are designed for the ‘purpose of sexual arousal’ aiming to capture those images which on face value may not appear sexual, but given the circumstances of an investigation it would appear they were designed for that purpose[147]. For example, images in naturist scenarios or those in circulation from publications which although may have a genuine purpose, have been collected by a suspect for the purpose of sexual arousal. Although in theory, this approach may seem sensible as it ensures a wider definition with the ability to potentially prosecute more offenders in possession of material of this type, practically, it leads to further complexity in judging whether an image was meant to be sexual. Holmes and Holmes’s conception is vague, yet it does highlight a controversial area of debate, which Taylor and Quayle highlight the extent of this issue stating ‘even non-sexualised images may be used as an aid to masturbatory fantasy as well as a prelude to actual sexual activity with children’[148]. Therefore determining whether an image of a child was designed to be sexual involves determining the mind-set of the possessor, an arguably impossible task, and one that must be tackled on a case-by-case basis.

The task of distinguishing IDCSA in order to constitute an offence remains a grey area. Although there is a general perception that IDCSA contain some form of sexual pose or content, there is little elaboration on what constitutes this from the definitions examined above. Some clarity on this point has been provided by laws in foreign jurisdictions (albeit non-binding in England and Wales) and provides a starting point when considering if material is to be determined as IDCSA. First, in the American case of *Dost*[149], a test for determining IDCSA was developed based on the concept of ‘lasciviousness' noting six key factors for establishing whether a given image is IDCSA which are expanded upon by through academic comment from Gillespie [150]:

1. Whether the focal point of the visual depiction is on the child's genitalia or pubic area;
2. Whether the setting of the visual depiction is sexually suggestive;

[147] S. T. Holmes & R. M. Holmes, *Sex Crimes Patterns and Behaviours* (1st, Sage Publications 2002) 291
[148] E. Quayle & M. Taylor, ‘Paedophiles, pornography and the Internet: Assessment issues.’ (2002) 32.7 British Journal of Social Work 863
[149] *US v Dost* 636 F.Supp.828 (1986)
[150] A. A. Gillespie, 'Defining Child Pornography: Challenges for the Law' (2010) 22 Child & Fam. L. Q. 200, 210

3. Whether the child is depicted in an unnatural pose;
4. Whether the child is fully or partially clothed or nude;
5. Whether the visual depiction suggests sexual coyness or a willingness to engage in sexual activity;
6. Whether the visual depiction is intended or designed to elicit a sexual response in the viewer

Further, the Canadian case of *Sharpe*[151] provided a two-stage test, which has been placed in context by Gillespie:

> First, when looked at objectively and in its context, did its dominant characteristic appear to be the depiction of the child's sexual organ or anal region? The reference to 'dominant characteristic' means that it must be the main (but not necessarily the only) characteristic of the picture. If that test is satisfied then the second test relates to its purpose and the question to be asked is whether it will be 'reasonably perceived as intended to cause the sexual stimulation of the viewers'[152].

To provide additional clarity on this issue, the Combatting Paedophiles Information Networks in Europe Centre (COPINE) attempts to specify additional guidance on the types of image which may be contemplated as sexual and therefore constitute IDCSA, through the development of the COPINE scale[153]. COPINE was a joint project between the University of Cork and the Paedophile Unit in the Metropolitan police to develop a classification for IDCSA and to understand the types of imagery collected by paedophiles[154]. The problems posed by defining IDCSA impacts upon the assessment of the severity of the act carried out by the defendant and ultimately sentencing. The COPINE project aims to assist in the identification of IDCSA noting that images exist on a continuum, ranging in severity, which depict the level or obsession or involvement that the offender has with this type of material[155].

The COPINE scale is "a scale of decency which had been created in Ireland for categorising the severity of images of child sexual abuse."[156]. Consisting of ten levels, it is designed to identify the seriousness of the image depicting the abuse and the accompanying text based descriptions provide a useful guide when attempting to provide a definition of IDCSA. For

[151] *R v Sharpe* 2001 SCC 2.
[152] A. A. Gillespie, 'Defining Child Pornography: Challenges for the Law' (2010) 22 Child & Fam. L. Q. 200, 210
[153] T. Krone, 'A typology of online child pornography offending' (2004) Australian Institute of Criminology
[154] E. Quayle & M. Taylor, 'Paedophiles, pornography and the Internet: Assessment issues.' (2002) 32.7 British Journal of Social Work 863 and R. Cohen-Almagor, 'Online Child Sex Offenders: Challenges and Counter-Measures.' (2013) 52.2 The Howard Journal of Criminal Justice 190
[155] E. Quayle 'The COPINE project.' (2008) 5 Irish Probation Journal 65, 67
[156] *R. v Dodd (Jonathan James)* [2013] EWCA Crim 660

example, level one images, references as indicative, are those that are "non-erotic and non-sexualised pictures showing children in their underwear, swimming costumes etc. from either commercial sources or family albums. Pictures of children playing in normal settings, in which the context or organisation of pictures by the collector indicates inappropriateness"[157]. In contrast level 10 images, termed Sadistic or bestiality include "pictures showing a child being tied, bound, beaten, whipped or otherwise subject to something that implies pain or; Pictures where an animal is involved in some form of sexual behaviour with a child"[158].

The COPINE scale brings us one step closer to tackling the issues raised by Holmes and Holmes[159] earlier through the introduction of an 'indicative' category of IDCSA, recognising the need to subjectively assess a potential offender's mind-set and reasoning behind having any material of this type. The definitions provided by the COPINE project are designed to ensure consistency in sentencing and to highlight the severity of the IDCSA, which the offender has engaged with. However, in 2002, the Sentencing Advisory Panel England and Wales moved to condense the scale, removing levels one to three arguing that such photos were not symptomatic of indecency[160]. The case of *Oliver*[161] provided a precedent in England and wales (until 2014) for determining the seriousness of the offence of IDCSA by categorising IDCSA, specifically in relation to the nature of the material and the extent of the offender's involvement. The nature of the material was to be determined with regards to the following five levels:

1. Images depicting erotic posing with no sexual activity;
2. Sexual activity between children, or solo masturbation by a child;
3. Non-penetrative sexual activity between adults and children;
4. Penetrative sexual activity between children and adults;
5. Sadism or bestiality.

Although *Oliver*[162] provides guidance for the sentencing of offenders, it subsequently provides guidance for the definition of the types of IDCSA in England and Wales in absence of any set by domestic legislation. Therefore through reference to *Oliver*[163], England and Wales had access to an in-direct objective definition of forms of IDCSA. Yet in 2014, The

[157] E. Quayle 'The COPINE project.' (2008) 5 Irish Probation Journal 65, 67
[158] E. Quayle 'The COPINE project.' (2008) 5 Irish Probation Journal 65, 67
[159] S. T. Holmes & R. M. Holmes, *Sex Crimes Patterns and Behaviours* (1st, Sage Publications 2002) 291
[160] E. Quayle 'The COPINE project.' (2008) 5 Irish Probation Journal 65, 69
[161] *R. v Oliver (Mark David)* [2002] EWCA Crim 2766;
[162] *R. v Oliver (Mark David)* [2002] EWCA Crim 2766;
[163] *R. v Oliver (Mark David)* [2002] EWCA Crim 2766;

Sentencing Council's Sexual Offences Definitive Guidelines have since amended the categories previously defined in *Oliver*[164], producing the following three categories, from which IDCSA can fall into in England and Wales:

- Category A: An image depicting penetrative sexual activity and sexual activity with an animal or sadism.
- Category B: An image depicting non-penetrative sexual activity.
- Category C: Any other indecent images not falling within categories A or B. [165]

Despite the various implementations of IDCSA definitions, one thing which each attempts to capture is those images which depict acts of abuse that have ultimately caused harm to the child, a founding arguments for the regulation of IDSCA and criminalising possession of this material. It is clear that from the descriptions provided by *Oliver*[166] and the COPINE scale that the acts depicted in IDCSA falling within those categories cause severe harm to the child victim. Therefore, the following section will examine the concept of harm caused to the child who is depicted in this form of illegal imagery and the reasons behind using this as a justification for regulating IDCSA.

2.2 Prevent Harm to the Child

One of the founding justifications for preventing the creation, distribution and possession of IDCSA surrounds the notion of harm which is caused by the material, both in its production and through its distribution and viewing by others[167]. This section will examine the harm caused to the child depicted.

Aries[168] notes that in medieval cultures the concept of childhood did not exist blurring the distinction between the adult and child. Children living during this time were more likely to be subject to sexual abuse and other forms of ill treatment leading to the production of records documenting the acts[169]. The concept of childhood is considered relatively new and Corby[170] suggests that a greater degree of protection for children began to be established at the beginning of the 19th century. It is now arguable that children enjoy the greatest

[164] *R. v Oliver (Mark David)* [2002] EWCA Crim 2766;
[165] Sentencing Council. Sexual Offences Definitive Guideline. (2013) <https://www.sentencingcouncil.org.uk/wp-content/uploads/Final_Sexual_Offences_Definitive_Guideline_content_web1.pdf> accessed 11 June 2015
[166] *R. v Oliver (Mark David)* [2002] EWCA Crim 2766;
[167] C. B. Hessick 'The Limits of Child Pornography' (2014) 89 Ind. LJ 1437
[168] P. Aries *Centuries of Childhood* (1st, Penguin 1962) 125
[169] L. De Mause *The History of Childhood* (1st, Souvenir Press 1976)
[170] B. Corby *Child Abuse Towards a Knowledge Base* (1st, Open University Press 1993)

protection they have ever been afforded. Within society, children enjoy a highly protected status and are perceived as innocent and vulnerable individuals, fundamentally dissimilar to adults, who must be protected from harm[171]. Such sentiments were echoed in *O'Brien*[172], where Justice Cox stated that the sexual abuse offence that had been committed had 'stolen the victims childhood and innocence'. Kleinhans suggests "childhood and sexuality are western sacred cows of the present age. When combined in the form of 'childhood sexuality', the result is invariably a taboo strong enough to ward off all but the very persistent" [173]. Despite this, as identified in Chapter 1, there are wide spread accounts of individuals continuing to abuse children in order to produce illegal imagery.

The need to develop such intolerance for these acts lies with theories surrounding the creation and use of this illegal material. A fundamental argument stems from a need to prevent the original abuse depicted in any captured sexualised content. As Ramirez[174] indicates, often the abuse suffered by a child is not a singular event; it is one of a number, which can span across a number of weeks, months and years. Those under the age of 16 who are involved in this form of abuse are incapable of providing informed or legal consent to such sexual acts and therefore the pictures produced stand as a permanent representation of the abuse[175]. Further, it is argued that every time the material is viewed in the future is a continuation of the original abuse and serves as a permanent source of embarrassment and distress for the original child victim[176].

Where a child has been involved in acts leading to the production of IDCSA there is both physical and mental harm to the child[177]. Speaking in the House of Lords, Baroness Seccombe noted that "such early experience of sexual activity often leaves deep emotional scars on a child which can damage future relationships. Furthermore, the child must live with the permanent knowledge that pictures of the abuse are still circulating"[178]. Comments

[171] S. Ost, *Child Pornography and Sexual Grooming: Legal and Societal Responses* (1st, Cambridge University Press 2009) 273
[172] *Regina v Paul Andrew O'Brien* [2006] EWCA Crim 3339 at 10
[173] M. M. Kleinhans, 'Criminal justice approaches to paedophilic sex offenders.' (2002) 11.2 Social & Legal Studies 233, 233
[174] J. A. Ramirez, 'Propriety of internet restrictions for sex offenders convicted of possession of child pornography: should we protect their virtual liberty at the expense of the safety of our children?.' (2014) 12 Ave Maria L. Rev. 123
[175] P. Jenkins, *Beyond Tolerance: Child Pornography on the Internet* (1st, NYU Press 2003) 260
[176] HC Deb 08 May 2002 vol 385 c233W
[177] D. D. Burke, 'The Criminalization of Virtual Child Pornography: A Constitutional Question' (1997) 34 Harv. J. on Legis. 439
[178] HL Deb 04 October 2000 vol 616 cc1564-89

from Silbert[179] suggests that the effects of being a victim of child sexual abuse are felt more in the long term, arguably when the individual has reached maturity and is able to fully comprehend what has happened and the impact of knowing the material is in circulation, "haunting" the victim[180] with the knowledge that it has the potential to resurface[181].

There is limited scope to argue that a child depicted within IDCSA is not subject to harm both in their short and long-term development. As Cassell *et al.* state, due to the IDCSA subsequently produced by the abuse, the original act of "sexual abuse is only the beginning of a lifetime of despair" [182]. Given this, those who possess and actively seek to possess IDCSA are continuing the abuse process and increasing the harm incurred by the original child victim by encouraging IDCSA to remain in circulation.

However, it is not just the child that is subject to harm, and the position that society could be harmed via IDCSA must be considered. The following section examines the notion of harm caused to society through the widespread availability and production of IDCSA.

2.3 The Harm to Society by IDCSA

When material is viewed which contests the notion of childhood innocence it causes shock and distress[183]. It is arguably safe to infer that the majority of those within society have never seen IDCSA or wish to view it. Yet, if we fail to regulate IDCSA, this may lead to a rise of accessible IDCSA hosted on the Internet. This in turn may increase the chance of individuals stumbling across IDCSA when browsing the Internet. In such an instance, viewing this content is likely to cause distress. Additionally, an increased availability of IDCSA may encourage those who are inquisitive, to pursue additional material of this type, particularly when coupled with the knowledge that they may perceive themselves to be anonymous

[179] M. H. Silbert, 'On Effects on Juveniles of Being Used for Pornography and Prostitution' (1989), in D. Zillman & Bryant, C. (eds.), *Pornography: Research Advances and Policy Considerations, (*Hillside, NJ: Lawrence Erlbaum)

[180] D. D. Burke, 'The Criminalization of Virtual Child Pornography: A Constitutional Question' (1997) 34 Harv. J. on Legis. 439

[181] R. Michaels, 'Criminal Law-The Insufficiency of Possession in Prohibition of Child Pornography Statutes: Why Viewing a Crime Scene Should Be Criminal.' (2008) 30 W. New Eng. L. Rev. 817, 818

[182] P. G. Cassell, J. R. Marsh & J. M. Christiansen, 'Case for Full Restitution for Child Pornography Victims, The.' (2013) 82 Geo. Wash. L. Rev. 61.

[183] S. Ost, *Child Pornography and Sexual Grooming: Legal and Societal Responses* (1st, Cambridge University Press 2009) 12

when operating online[184]. Failure to condemn IDCSA subsequently provides justification for this act, providing those involves with a greater audience in which to impose this material on[185].

Failure to prohibit IDCSA may intensify general curiosity surrounding the material, prompting individuals to actively search for IDCSA in absence of any legislative deterrents. The problem this causes is two-fold. First, if demand, driven by curiosity increases, so may the volume of child abuse acts carried out in order to create new material[186]. Second, concerns surround those who view IDCSA, their underlying motive and potential to escalate their involvement in the abuse[187].

It is arguable that if more individuals engage in possessing IDCSA, as a consequence, there is an inferred increase in the chance that those individuals will participate in the sexual abuse of a child, although definitive links have yet to be established. However this concern requires further analysis, which is provided in the following section.

2.4 Types of Offender and Escalation of Abuse

Additional concerns for justifying the regulation of possession of IDCSA resonate from arguments surrounding the *modus operandi* of the offender and suggest IDCSA acts as a stimulus for individual to progress their interest from purely viewing to carrying out actual forms of physical child abuse[188]. Akdeniz[189] describes the following hierarchy of participants involved within IDCSA offences. Although all forms of involvement in IDCSA offences are seen as grave, three distinctive roles are proposed, the creator, distributor and collector.

[184] G. Horsman, 'The challenges surrounding the regulation of anonymous communication provision in the United Kingdom.' (2016) 56 Computers & Security 151

[185] E. Quayle & M. Taylor, 'Child pornography and the Internet: Perpetuating a cycle of abuse.' (2002) 23.4 Deviant Behavior 331

[186] J. Wolak, D. Finkelhor & K. J. Mitchell, *Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study* (Crimes against Children Research Center, 2005) and M. Wells *et al.* 'Defining child pornography: Law enforcement dilemmas in investigations of Internet child pornography possession' (2007) 8.3 Police Practice and Research 269 and I. A. Elliott & A. R. Beech, 'Understanding online child pornography use: Applying sexual offense theory to internet offenders.' (2009) 14.3 Aggression and Violent Behavior 180

[187] E. Quayle & M. Taylor, 'Child pornography and the Internet: Perpetuating a cycle of abuse.' (2002) 23.4 Deviant Behavior 331

[188] P. Jenkins, *Beyond Tolerance: Child Pornography on the Internet* (1st, NYU Press 2003) 260

[189] Y. Akdeniz, *Internet Child Pornography and the Law: National and International Responses* (1st, Ashgate Publishing 2013) 326

Quayle[190] expands upon these roles and adds a fourth entitled 'Internet solicitor', those that actively seek to groom victims on-line for the purposes of sexual abuse. This thesis proposes that another role is added, that of the 'looker'; an individual who seeks to passively view the material on line and deliberately not to acquire any ownership over it, using protocols like online streaming. Those who 'just look' are analogous to the possessor, only they do not take physical possession of an image, effectively only possess the visual image of it with no intention of collecting and storing the content.

Those that create authentic original (not copies or computer generated) IDCSA are directly involved in the original abuse or instigate the events involved and are often subject to the most severe statutory punishment. These individuals are arguably the most dangerous as they are in physical contact with the child victims and instigate the abuse in order to produce new IDCSA, potentially for monetary gain. Distributors are those who actively spread the illegal media and arguably feed the desire to possess and view this content. Motives for distributing IDCSA may not simply surround sexual desires, but financial rewards must also be considered. In addition, due to technological developments in digital imagery, distributors may well create new instances of original material. It should be noted that roles may overlap and individuals may escalate their involvement in offences because of the ease that digital imagery can be created and shared. Finally, those who seek to collect and possess IDCSA frequently operate separate to the original physical sexual abuse, seeking to feed an interest in the illegal act and are the focus of this thesis.

As of the *CJA88*, possession in the England and Wales is illegal and this offence forms the focus of this research. Sullivan and Beech[191] expand on the role of a possessor and establish the following three key motivations behind those who seek to possess IDCSA. Those who collect as part of a wider range of sexual offending, those who seek to fuel an erotic interest and those who are curious, with all roles arguably feeding the demand for IDCSA to be produced. The possession of IDCSA may seek to desensitise an offender to the nature of their actions[192], and research suggests that prolonged exposure to this content may prevent the viewer from realising the harm that is being depicted[193]. In addition, technological

[190] E. Quayle, 'The COPINE project.' (2008) 5 Irish Probation Journal 65, 74
[191] J. Sullivan & A. Beech, 'Assessing internet offenders' (2004) In M. Calder (Ed.) *Child sexual abuse and the internet: Tackling the new frontier* 69 (UK Russell House Publishing Ltd)
[192] L. M. Jones, 'Regulating Child Pornography on the Internet - The Implications of Article 34 of the United Nations Convention on the Rights of the Child' (1998) 6 Int'l J. Child. Rts. 55, 57
[193] D. Linz, E. Donnerstein & S. M. Adams, 'Physiological desensitization and judgments about female victims of violence.' (1989) 15.4 Human Communication Research 509

developments have created a previously unforeseen problem by blurring the lines between those that simply possess and those that distribute and create[194]. As images can easily be duplicated and shared via electronic communications or peer-to-peer applications, an offender can quickly and easily escalate their involvement in these harmful activities from possessor to distributor. Similarly, photographic editing software can offer the facilities for offenders to create new IDCSA.

An offender's possessed IDCSA may be fuelling their desire to escalate their involvement in child sexual abuse. In doing so, the possessor may reach a point where they actively seek to sexually abuse children[195]. Levy indicates that possessors of IDCSA may also utilise the images to attract potential child victims online by attempting to encourage the child to believe that sexual acts are normal behaviour and that they should engage in them[196]. Further, possessors may converse with fellow possessors online to support each other's obsession with IDCSA, ultimately encouraging these acts, providing each with a sense of justification[197]. Krone[198] states that more research is needed surrounding whether an individual involved in the possession of IDCSA leads to the actual physical sexual abuse of children, and although there is no definitive link, it remains an area of concern. Although there is little evidence to conclusively suggest that viewing IDCSA leads to an offender committing actual sexual abuse[199], Calder[200] suggests that the aspiration for an offender to carry out the abuse is implicit. Further, the risk of exposing children to further abuse by allowing offenders to possess and view this material is arguably too great.

Statistics depicting offender involvement in child offences are difficult to locate, of those which are available, research often takes place in the US or Canada. However those studies which can be identified, despite being historic, still endorse current concerns. Figures

[194] E. Quayle & M. Taylor, M., 'Paedophiles, pornography and the Internet: Assessment issues.' (2002) 32.7 British Journal of Social Work 863

[195] Y. Akdeniz, *Internet Child Pornography and the Law: National and International Responses* (1st, Ashgate Publishing 2013) 326

[196] N. Levy, 'Virtual child pornography: The eroticization of inequality.' (2002) 4.4 Ethics and Information Technology 319

[197] N. Levy, 'Virtual child pornography: The eroticization of inequality.' (2002) 4.4 Ethics and Information Technology 319

[198] T. Krone, 'A typology of online child pornography offending' (2004) Australian Institute of Criminology

[199] L. Webb, J. Craissati & S. Keen, 'Characteristics of Internet child pornography offenders: A comparison with child molesters.' (2007) 19.4 Sexual abuse: a journal of research and treatment 449

[200] M. Calder, 'The internet: Potential, problems and pathways to hands-on sexual offending' (2004) In M. Calder (Ed.) Child sexual abuse and the internet: Tackling the new frontier 2 (Russell House Publishing Ltd)

provided from the National Centre for Exploited Children[201] (of US origin) show that 40% of those surveyed were classed as dual offenders and possessed IDCSA and carried out acts of child sexual abuse. Of the 53% of offenders who possessed or distributed IDCSA, 31% of those were involved in child sexual victimisation. Research from Wolak[202] provided that from approximately 2577 arrests recorded in the US in 2000 for crimes of Internet sexual abuse against children, 83% possessed IDCSA depicting children between the ages of six and twelve. Studies into the characteristics of IDCSA possessors are limited but from those available the following comments are drawn. The 2001 study from Burke *et al*.[203] suggests offenders tend to be within the age bracket of 25-50. Research complete within the US suggest that those involved in child sexual abuse image offences are frequently Caucasian males above the age of twenty six[204]. Additional characteristics include those who are intelligent with a high degree of education that are generally in employment[205] however, such studies fail to provide generalisable and reliable results. Carr and Hilton[206] indicate that a greater volume of research needs to be carried out to establish the risks poses by those who possess IDCSA. Current studies are limited by small sample sets and varying legislative content, which restrict access to offender history[207]. The historic comments of Fontaine[208] remain relevant, as at present the characteristics of the abuser have still yet to be definitively established and due to limitations in previous studies it cannot be said with certainty that the characteristics of those arrested and surveyed are representative of the abuser population. Conversely one must consider the controversial view that IDCSA may actually maintain a positive role in protecting children, which merits brief discussion. Although unsupported through empirical studies, it could be argued that IDCSA prevents the number of acts of child sexual abuse from increasing as offenders may find the images themselves sufficient to satisfy their interest. However, just as noted with previous study

[201] J. Wolak, D. Finkelhor & K. Mitchell, *Child-pornography possessors arrested in internet-related crimes: findings from the National Juvenile Online Victimization Study*. (Alexandria, VA: National Center for Missing & Exploited Children, 2005)
[202] J. Wolak, D. Finkelhor & K. Mitchell, *Child-pornography possessors arrested in internet-related crimes: findings from the National Juvenile Online Victimization Study*. (Alexandria, VA: National Center for Missing & Exploited Children, 2005)
[203] A. Burke, S. Sowerbutts, S. Blundell & M. Sherry, 'Child pornography and the internet: Policing and treatment issues.' (2001) 9.1 Psychiatry, Psychology and Law 79
[204] J. Wolak, D. Finkelhor & K. Mitchell, *Child-pornography possessors arrested in internet-related crimes: findings from the National Juvenile Online Victimization Study*. (Alexandria, VA: National Center for Missing & Exploited Children, 2005)
[205] A. Burke, S. Sowerbutts, S. Blundell & M. Sherry, 'Child pornography and the internet: Policing and treatment issues.' (2001) 9.1 Psychiatry, Psychology and Law 79
[206] J. Carr & Z. Hilton 'Combatting Child Abuse Images on the Internet' in J. Davidson, P. Gottschalk (eds), *Internet Child Abuse Current Research and Policy* (1st, Routledge 2011).
[207] J. Carr & Z. Hilton 'Combatting Child Abuse Images on the Internet' in J. Davidson, P. Gottschalk (eds), *Internet Child Abuse Current Research and Policy* (1st, Routledge 2011) 54
[208] J. L. Fontaine, *Child Sexual Abuse* (1st, Polity Press 1990) 108

limitations, characteristics found in offender behaviour are yet to be conclusively established. A study from Endrass *et al*. of 231 men charge with IDCSA offences showed no conclusive link between possessing IDCSA and carrying out child sexual abuse[209].

2.5 A Brief Consideration of Counter Arguments

Hessick[210] proposes somewhat controversial arguments surrounding those who possess IDCSA. It is suggested that due to the Internet and the abundance of IDCSA hosted on it coupled with ease of access, those who possess IDCSA now pose less of a threat than offenders pre-dating the Internets use. Justification for this suggestion surrounds the simplicity of acquiring IDCSA. Before the Internet, offenders expended significant effort to obtain IDCSA demonstrating a higher degree of obsession and determination. These traits arguably provide a higher risk of the user escalating their interest towards acts of sexual abuse of children. Yet using the Internet, Hessick[211] suggests simple curiosity may be an underlying motivation or even as a means of using the pictures as a way of developing relationships with other adults online. Essentially, Hessick[212] argues the potential for the Internet to have reduced the blameworthiness of possession offenders due to an inability to assess the risks associated with the illegal material. In addition, Levy contemplates the position that accessing imagery may supress acts of physical sexual abuse, yet it was acknowledged that definitive analysis of this claim was unavailable and currently remains unfounded[213].

2.6 Concluding Thoughts

Chapter 2 has presented an examination of the harm caused by IDCSA, drawing attention to the different roles an offender can take in these offences. IDCSA causes significant harm to the original child victim, both physically and mentally, providing strong justifications for its regulation. Although many roles exist in the implementation of IDCSA related offences, it is arguable that the possessor is one of the main catalysts for the growth of this material. Possessors likely drive the demand for IDCSA, the production of new material, and, ultimately increase the volume of acts of sexual abuse with the want for new material. Possessors prolong the lifespan of material in circulation, exacerbating the harm and

[209] J. Endrass, F. Urbaniok, L. C. Hammermeister, C. Benz, T. Elbert, A. Laubacher & A. Rossegger, 'The consumption of Internet child pornography and violent and sex offending.' (2009) 9.1 BmC Psychiatry 43

[210] C. B. Hessick, 'Disentangling child pornography from child sex abuse.' (2010) 88 Wash. UL Rev. 853

[211] C. B. Hessick, 'Disentangling child pornography from child sex abuse.' (2010) 88 Wash. UL Rev. 853

[212] C. B. Hessick, 'Disentangling child pornography from child sex abuse.' (2010) 88 Wash. UL Rev. 853

[213] N. Levy, 'Virtual child pornography: The eroticization of inequality.' (2002) 4.4 Ethics and Information Technology 319

embarrassment caused to the child. Although links towards escalation are inconclusive, this thesis supports the views of Calder[214], who indicates those who seek to view this form of material are also likely to harbour thoughts and desires to physically participate in this behaviour. There is a need to regulate IDCSA in order to prohibit and deter access to it, preventing an offender from possessing it. Stopping access to the material may decrease the demand for it, which would ultimately lead to a decrease in production of the material and acts of child abuse from which the images originate from. In addition, effective regulation stands to prevent the normalisation of IDCSA, ensuring that the presence of it in today's society is not tolerated and the harm caused by it continues to be acknowledged. However, as previously discussed, statistics show that IDCSA offences are still prevalent. In addition, many offences remain unreported or have not been identified due to the methods now used for accessing IDCSA.

As identified in Chapter 1, the majority of possessors of IDCSA now maintain this material in digital form. To prosecute for possession offences, the challenge to law enforcement now focuses on establishing possession of intangible digital data. The offence is now fundamentally different from those witnessed at the time of the enactment of the CJA88, yet legislations recognition of the evolution has been relatively slow to adapt. Chapter 3 will therefore analyse the development of UK legislation surrounding IDCSA offences and available defences, providing an underpinning knowledge of this area of law.

[214] M. Calder, 'The internet: Potential, problems and pathways to hands-on sexual offending' (2004) In M. Calder (Ed.) 'Child sexual abuse and the internet: Tackling the new frontier' 2 (UK, Russell House Publishing Ltd)

Chapter 3

The Development of Law Governing IDCSA In England and Wales.

3.1 Introduction

In Chapter 2, the harms posed to society and child abuse victims by IDCSA have been highlighted, providing justification for England and Wales's regulation of this material. As a result of concerns over the increased volume of this material in circulation and its links to child abuse, expressed both in Parliament[215] and the media[216], the introduction of legislation directly targeting IDCSA was first witnessed in 1978, despite this type of material being in existence long before this date. Now, some 38 years after the enactment of the PCA78, the challenges faced when regulating IDCSA are fundamentally different to those that were initially envisaged. When coupled with technological developments, offending behaviour in this area of law has now been revolutionised, where issues range from the transition from physical paper-based photographs to digital images, to the complexity of computer systems providing access to the Internet and online forms of IDCSA.

Chapter 3 provides an analysis of these regulations by chronologically examining legislative developments surrounding IDCSA in England and Wales. The Chapter will commence with a discussion of the Obscene Publication Acts, before proceeding to highlight incremental changes in law and current precedents. The aim of this chapter is to provide an in-depth understanding of this area of law, providing a foundation of knowledge from which the thesis can build upon as it focuses on the offence of possession of IDCSA and the intricacies of digital data in Chapters 4 and 5.

3.2 The Obscene Publications Act (OPA) 1959 and 1964

Prior to 1978, domestic legislation directly addressing IDCSA did not exist in English law; instead reliance was placed upon the Obscene Publication Acts 1959 and 1964, which provide the starting point for discussions in this chapter. Before the widespread use of the

[215] HC Deb 17th November 1977, Vol 939, col 737-978

[216] J. Harrison, 'Whitelaw urges child porn blitz.' *Daily Mail* (London, 15 November 1977) accessed 28 February 2015 and A Staff Reporter, 'Mrs Thatcher urges action over child pornography.' *Times* (London, 6 September 1977) accessed 28 February 2015.

Internet, the Obscene Publication Acts 1959 and 1964 were the main tools for dealing with what was termed obscene content[217]. Although the OPA's preamble indicates that its aim was to strengthen laws concerning pornography, it must be noted that the OPA was not put in place to regulate pornography alone, but for any material, which is deemed obscene[218] (demonstrated by *John Calder Publications Ltd*[219] where the obscenity of literature regarding drug taking was examined). In the lead up to the enactment of the OPA, attentions were focused on the suppression of general pornographic content[220], with no commentary directly addressing IDCSA both in media and Parliamentary discussion. It is arguable that at this point, the problem of IDCSA was unforeseen, yet literary records describing acts of child abuse were not. As a result, booksellers were subject to increasing attention regarding the material they were retailing, and ultimately whether the content of the books they sold were deemed obscene under the OPA[221].

At the heart of arguments for invoking obscenity legislation in relation to child abuse was the publication of 'Lolita', a novel focusing on a man's obsession with a 12-year-old girl, with suggestions made for the potential for such literature to corrupt those who read it[222]. As a result, written articles were deemed the main pornographic threat in need of regulation[223], with subsequent books such as '*Fanny Hill*' invoking similar levels of scrutiny in 1964 due to its supposed pornographic descriptions[224]. Following growing media outcry regarding an perceived increasing volume of pornographic content in circulation and its potential to

[217] A. Nair & J. Griffin, 'The regulation of online extreme pornography: purposive teleology (in) action' (2013) 21.4 Int J Law Info Tech 329

[218] R. A. Elman, *Sexual Politics and the European Union: The New Feminist Challenge* (1st, Berghahn Books, 1996) 73

[219] *John Calder Publications Ltd v Powell* [1965] 1 QB 509

[220] Anon 'Obscene books Bill gets reading.' *Daily Mail* (London, 19 November 1958) accessed 21 February 2015 and Anon 'Changes Proposed In Law On Obscene Publications.' *Times* (London, 28 March 1958) accessed 21 February 2015

[221] Anon 'Changes Proposed In Law On Obscene Publications.' *Times* (London, 28 March 1958) accessed 28 February 2015 and A. Scotford *et al*. 'Now let's have a clean-up on the bookstalls.' *Daily Mail* (London, 18 April 1961) accessed 28 February 2015.

[222] C. Wilson, 'Where can I take Aunt Edna?' *Daily Mail* (London, 2 November 1959) accessed 21 February 2015 and K. Allsop, 'The row about Lolita.' *Daily Mail* (London, 18 December 1958) accessed 21 February 2015

[223] OUR CORRESPONDENT, 'Action Urged On Pornography.' *Times* (London, 29 December 1961) accessed 21 February 2015

[224] Anon, 'Author Says Novel 'Fanny Hill' Not Pornography.' *Times* (London, 21 January 1964) accessed 21 February 2015.

corrupt those who encounter it[225], the UK government opted not to restrict particular genres of pornography, but to prohibit material, which is deemed obscene using the OPA.

Obscenity is a significantly broad term covering more than the depiction of sexual acts[226], demonstrated in *Gibson*[227], where questions of obscenity were raised over the act of displaying earrings made from foetal tissue in a public gallery. Prior to the PCA78, the publication of what is now deemed IDCSA was regulated by the OPA with the main offence set out in Section 2(1) OPA as follows.

> "Subject as hereinafter provided, any person who, whether for gain or not, publishes an obscene article shall be liable"

Under Section 1(2), an article includes anything "containing or embodying matter to be read or looked at or both, any sound record, and any film or other record of a picture or pictures"[228]. For an article to be illegal it must meet the 'obscenity test' where it must "tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it" [229]. The legislation was not designed to prohibit or control pornography in general, only to police material, which depicted particularly grave scenes. The case of *Anderson*[230] established that material, which is only 'filthy' or 'lewd', would not fall within the confines of the legislation and to satisfy the test, material must have a propensity to deprave or corrupt[231]. Similarly in *Whyte*[232], shocking material was not covered. As a result, ambiguity surrounding what would constitute obscene materials given the test is subjective (subject to the personal opinions and judgements of those determining obscenity) and prone to varying moral standards apparent in different areas[233]. Cheng[234] states "the 'average man' or 'man in the jury box' called to judge whether materials are obscene does so from his character and conscience",

---

[225] Anon, 'Changes Proposed In Law On Obscene Publications.' *Times* (London, 28 March 1958) accessed 28 Feb. 2015 and A. Scotford, *et al*. 'Now let's have a clean-up on the bookstalls.' *Daily Mail* (London, 18 April 1961) accessed 28 February 2015.
[226] Y. E. Cheng 'Pornography: women matter' (2002) UCL Jurisprudence Review 144, 145
[227] *R. v Gibson (Richard Norman)* [1990] Crim. L.R. 738
[228] Obscene Publications Acts 1959, s 1(2)
[229] Obscene Publications Acts 1959, s1(1)
[230] *Anderson* [1972] 1 QB 304.
[231] *Martin Secker and Warburg* [1954] 2 AER 683.
[232] *DPP v Whyte* [1972] AC 849
[233] Y. Akdeniz, 'The regulation of pornography and child pornography on the Internet' (1997) The Journal of Information, Law and Technology 1, 1
[234] Y. E. Cheng 'Pornography: women matter' (2002) UCL Jurisprudence Review 144, 145

thoughts echoed by Fenwick[235] and Stone[236], as 'no one really knows what constitutes obscene material' in practice[237]. This sentiment is expanded upon by Samuels[238] who states, "if the matter comes before a jury there is likely to be a high degree of publicity" and in turn the jury's verdict is likely unpredictable[239].

Although the application of the obscenity test may prove troublesome in certain cases, it would be difficult to envisage much of what is now considered IDCSA (although content which would score lower on the COPINE scale may prove troublesome) failing to sit within its confines, and therefore it is not the test itself that provides the main concern surrounding the OPA. Rather, it is its restricted application, which is problematic. Although the definition of an article is wide, the offence contained within the OPA is limited, where only publication is prohibited. Following Section 1(3) OPA publication occurs 'where an individual distributes, circulates, sells, lets on hire, gives, or lends it, or who offers it for sale or for letting on hire, shows, plays or projects it'[240]. An offence of mere private possession is omitted, and only when possession with intent to publish is established, is an offence committed[241]. In addition, the OPA fails to prohibit creation of obscene material. This left a significant gap in the law, allowing individuals to legally create material for personal use, which if published, would be illegal.

As Nair and Griffin[242] state the OPA were designed to only focus on the 'distributor of content', not the collectors and end-users. Arguably, the motive for the OPA only prohibiting publication of obscene material is best addressed by Rowbottom[243] who states the following;

> "Stopping the material being distributed in the first place will clearly be more efficient than trying to control it once it has been widely disseminated. The number of producers and distributors will be fewer than the potential

[235] H Fenwick, *Civil Liberties and Human Rights* (4th, Routledge 2009) 583
[236] R. Stone, *Textbook on Civil Liberties and Human Rights* (10th, Oxford University Press 2014) 355
[237] C. McGlynn & E. Rackley, 'Criminalising extreme pornography: a lost opportunity' (2009) 4 Criminal law review 245, 246
[238] A. Samuels, 'Obscenity and Pornography' (2009) JPN 187
[239] S. Easton, *The Problem of Pornography: Regulation and the Right to Free Speech* (1st, Routledge 2005) 132
[240] Obscene Publications Acts 1959, s 1(3)
[241] J. Rowbottom, 'Obscenity laws and the internet: targeting the supply and demand' (2006) Crim. L.R. 97, 98
[242] A. Nair & J. Griffin, 'The regulation of online extreme pornography: purposive teleology (in)action' (2013) 21.4 Int J Law Info Tech 329
[243] J. Rowbottom, 'Obscenity laws and the internet: targeting the supply and demand' (2006) Crim. L.R. 97, 98

> possessors of the material. The producer and distributor also take greater responsibility for the harms caused by such obscene material."

The decision to focus exclusively on prohibiting publication must also be considered against technological advances and society's stance regarding IDCSA in that era, the 1960s. It was not until the 1970s that the true severity of IDCSA and child abuse was beginning to be understood, undoubtedly a factor in the government's failure to directly address IDCSA offences prior to this time[244]. In addition, as noted in Chapter 1, pornographic material at this time was predominantly in the form of paper-based publications, (backed by media reports at this time[245]) with the widespread use of digital imagery arguably not yet envisaged. This form of media is difficult to produce and duplicate, with additional speed and cost implications, despite reports that from 1961-1964, Scotland Yard seized around five hundred thousand magazines, which breached the OPA[246]. In absence of technology such as the Internet and personal computers (which were mainly confined to the defence industry and business sector[247]), it was difficult to imagine the mass distribution of IDCSA or the hoarding of this material by individuals at this time. Perhaps a central argument lay with the perceived (and potentially accurate) view that limited obscene material (specifically IDCSA) was in existence at that time (thoughts also echoed some 15 years later[248]). Therefore as a result, prohibiting the publication of IDCSA alone may have been viewed as a sufficient method of stemming access to it and further creation of the material. However, the following subsequent conflicting sentiment was expressed by Lady Kinloss[249] in the House of Lords which retrospectively highlighted an apparent weakness with the OPA.

> It would seem that the 1959 Act is not as strong as it might be. I understand that magistrates frequently order confiscation and destruction of material—books, magazines, films and video tapes—but the retailers very quickly re-stock, as profits are so great and there are large supplies of the material.

The OPA remained the main tool for regulating IDCSA for some 15 years before the UK government introduced the Protection of Children Bill, regarded as a "finger-in-the-dyke", protecting the UK against an impending flood of IDCSA[250]. Subsequently, the PCA78 was enacted.

---

[244] P. Jenkins, *Beyond Tolerance: Child Pornography on the Internet* (1st, NYU Press 2003) 260
[245] Anon, ''Jail filth tycoons'.' *Daily Mail* (London, 4 February 1964) accessed 21 February 2015.
[246] Anon 'Scotland Yard Looks Into Mail Order Pornography.' *Times* (London, 2 September 1964) accessed 21 February 2015.
[247] R. Rojas & U. Hashagen, *The First Computers: History and Architectures* (1st, MIT Press 2002) 18
[248] 1979/80 Cmnd. 7772 Home Office. Report of the Committee on Obscenity and Film Censorship
[249] HL Deb 25 March 1982 vol 428 cc1083-130
[250] HC Deb 10 February 1978,vol 943, col 1832-744 at 1837

3.3 The Protection of Children Act 1978

It was not for a further 14 years after the OPA that the next and arguably founding milestone for the regulation of IDCSA was established, with England and Wales opting to directly legislate on the prohibition of IDCSA[251]. Calls by the media had been made to extend the OPA to make sexual imagery, which directly depicts children illegal, with reports that the current government was devaluing the significance of harm caused by such material[252]. Wide spread public anxiety surrounding the use of children in sexualised material and the negative impact this has upon a child's wellbeing was beginning to be reported the media[253], along with increased public comment in favour of regulation from soon to be Prime Minister, Margaret Thatcher[254]. In addition, an increase in sexual offences against children during 1960's and 70's was being witnessed, with the number of people found guilty for gross indecency with a child increasing almost five-fold over this time period[255]. Further, concern surrounding the use of bribes to encourage parents to allow their children to engage in acts of sexual abuse in order to produce IDCSA led to calls for the implementation of tougher penalties[256]. However, comments from the Home Office Committee on Obscenity and File Censorship suggested that despite these concerns, doubt still existed as to whether there was an actual need for legislation governing IDCSA and in turn, whether the UK faced an issue with the material at all in absence of any empirical evidence[257].

Arguably, recognition of the need for legislation governing IDCSA was likely influenced by the US's position in the late 1970s, with recent amendments to legislation prohibiting IDCSA[258]. Despite the true scale of IDCSA at that time being largely unknown[259], similar to that witnessed today, social workers and child rights activist Baroness Faithful[260] stated that there were IDCSA in the UK 'which is-or has often been-private business: just one passing a

[251] J. Harrison, 'Whitelaw urges child porn blitz. *Daily Mail* (London, 15 November 1977) accessed 12 February 2015.
[252] R. Butt, 'Stamp it out, this abominable evil of using children for pornography.' *Times* (London, 24 November 1977) accessed 12 February 2015.
[253] Anon 'Mr Rees willing to see if law can be tightened to tackle child pornography.' *Times* (London, 18 November 1977) accessed 12 February 2015.
[254] A. Young, 'Ban child porn, demands 'shocked' Maggie.' *Daily Mail* (London, 6 September 1977) 12 February 2015 and R. Butt, 'Stamp it out, this abominable evil of using children for pornography.' *Times* (London, 24 November 1977) accessed 12 February 2015.
[255] HC Deb 10 February 1978,vol 943, col 1832-744 at 1833-1834
[256] J. Harrison, 'Whitelaw urges child porn blitz. *Daily Mail* (London, 15 November 1977) accessed 12 February 2015.
[257] 1979/80 Cmnd. 7772 Home Office. Report of the Committee on Obscenity and Film Censorship at 26
[258] HL Deb 5 May 1978, vol 391, col 527-670
[259] L. S. Smith, 'Private Possession of Child Pornography: Narrowing at-Home Privacy Rights' [1991] Ann. Surv. Am. L. 1011, 1013
[260] HL Deb 5 May 1978, vol 391, col 527-670

photograph to another'. Comments from Symon[261] suggested that around 80% of IDCSA was imported into the UK with concerns raised by Sir Bernard Braine MP[262] that IDCSA was becoming a billion dollar industry in the US. These comments must be approached with caution as in absence of a reliable system for monitoring and quantifying this IDCSA (something which we still have been unable to do with sufficient accuracy), are likely subject to media hype and speculation. Yet despite this, a general consensus suggested an increase in prevalence of IDCSA and concern over its potential links to paedophilia[263] leading to the enactment of the PCA78[264]. This was the first piece of domestic legislation in England and Wales directly designed to control and criminalise the acts of making, distributing and publishing this content, with punishment for the offences carrying a maximum sentence of three years imprisonment at the time[265]. Although IDCSA would almost certainly be classed as obscene by the OPA, the PCA78 was designed apprehend those who were taking and distributing illegal photographs as well as publishing them[266].

Section 1(1) of the PCA78 provided that it was an offence to take, or permit to be taken, distribute or show, to possess with intent to show or distribute, or publish IDCSA. From this enactment, three issues are raised and now analysed in turn.

3.3.1 Is taking, making?

The offence of taking under Section 1(1)(a) PCA78 not only covers those who directly take an IDCSA but those who allow an individual to take an image are also guilty of the offence. By making the act of taking an IDCSA for private purposes illegal, an apparent gap in legislation due to an omission of the OPA was closed, where previously only the publication of this material would likely be deemed obscene and therefore illegal, a move which was welcomed[267]. However, a key omission surrounded the distinction between taking and making. When examined, the PCA78 appeared to prohibit direct acts of interacting with a

[261] P. Symon, 'Home Office criticized on child pornography.' *Times* (London, 4 February 1978) accessed 21 February 2015.
[262] HC Deb 14 July 1978, Vol 953, col 1919-848
[263] G. Clark Political Correspondent, 'Tory call to strengthen law on child pornography.' *Times* (London, 15 November 1977) accessed 12 February 2015 and T. Gibbons, 'Computer generated pornography' [1995] International Review of Law, Computers & Technology 85, 85. and H. Noyes Parliamentary Correspondent, 'Vote not needed on child pornography Bill.' *Times* (London, 11 February 1978) accessed 12 February 2015.
[264] A. Antoniou, 'Possession of prohibited images of children: three years on' (2013) 77.4 J. Crim. L. 337, 338
[265] Protection of Children Act 1978, s 6(2)
[266] Anon 'Bill to control child pornography makes the law more effective.' *Times* (London, 6 May 1978) accessed 12 February 2015.
[267] Anon 'Bill to control child pornography makes the law more effective.' *Times* (London, 6 May 1978) accessed 12 February 2015.

child in order to take in IDCSA. Yet, the act of making an IDCSA, for example through means of copying it and therefore making a separate new IDCSA, is not prohibited (although the possessor of the original image is liable to distribution offences under the Act). The reasoning behind omitting to include acts of making within the PCA78 is again arguably due to limitations in technological advances at the time, where the only methods of creating an IDCSA were perceived to be that of 'taking' a physical photo. Presumably, in absence of the availability of devices capable of mass duplication of media (although early generation scanning devices did exist[268]), those who are directly involved in acts of child abuse resulting in the taking of IDCSA were considered to be the primary source of this material. Those making new IDCSA from existing content may not have been considered a threat and in turn, the 'making' of new IDCSA by means other than taking was overlooked. Such sentiments appear to have been echoed by Baroness Faithful[269], who indicated that threat of IDCSA came from the distribution of magazines, despite subsequently omitting to acknowledge the danger posed by those who copy and then distribute this content.

3.3.2 You can Possess but not Distribute

The second point to raise considers the omission of a possession offence. The enacted distribution offence covers those who directly distribute the images (either physical distribution through post or in person) as well as those who display an image to another. The act of showing is therefore classed as a distribution of the visual content of the IDCSA, as opposed to a physical transaction involving a particular image. Further clarification of the offence of distribution is given in Section 1(2) PCA78 that sets out the additional elements of the offence of distribution.

> PCA78 Section 1(2) - "For purposes of this Act, a person is to be regarded as distributing an indecent photograph if he parts with possession of it to, or exposes or offers it for acquisition by, another person."

What is key to note is the omission of an offence of private possession, with section 1(1)(c) deeming possession illegal, only when accompanied with the intention to distribute or show the content. Despite the PCA78 recognising the need to police IDCSA, it did not recognise those who privately possess IDCSA as a concern. Although this is now considered a significant omission, it must be considered in light of conflicting reports surrounding the

[268] A. Basta, N. Basta, & M. Brown, *Computer Security and Penetration Testing* (1st, Cengage Learning 2013) 64

[269] HL Deb 5 May 1978, vol 391, col 527-670

origins of IDCSA. Returning to comments from Symon[270], who quoted the Chief Constable of Manchester Police as estimating that 80% of material came from foreign territories (a statement reiterated by MP Cyril Townsend in Parliament[271]. This was backed by reports suggesting countries such as Germany, Denmark and Holland were key producers and importers of IDCSA into the UK[272]), and therefore it must be questioned why possession was not prohibited. As the publication, distribution and creation of IDCSA was occurring outside of UK law, those who seek to possess the material were still driving the IDCSA industry. Further, prohibiting possession would be the only way to target offenders resident in the UK. However some 5 days later, Symon[273] also quotes an un-named police officer as stating over 75% of IDCSA is home produced. Such conflicting reports indicate that an understanding of IDCSA at that time was limited and the source and quantity of the material remained relatively unknown.

3.3.3 What is a photograph?

The final point raised is a consideration of what constitutes a photo. The PCA78 concerns IDCSA, however the term photograph was narrowly defined in comparison to current developments in photographic imagery. Under Section 7 PCA78 the following guidance was provided;

> (2) References to an indecent photograph include an indecent film, a copy of an indecent photograph or film, and an indecent photograph comprised in a film.
>
> (3) Photographs (including those comprised in a film) shall, if they show children and are indecent, be treated for all purposes of this Act as indecent photographs of children.
>
> (4) References to a photograph include the negative as well as the positive version.
>
> (5) "Film " includes any form of video-recording.

Perhaps the most significant issue is the absence of recognition for electronic data stored on a form of digital storage media to constitute a photograph, an omission that is

[270] P. Symon, 'Home Office criticized on child pornography.' *Times* (London, 4 February 1978) accessed 21 February 2015.
[271] HC Deb 10 February 1978,vol 943, col 1832-744
[272] Anon, 'Second reading for Bill to curb child pornography: Tory MP speaks of growing public anxiety.' *Times* (London, 11 February 1978) accessed 28 February 2015 and R. Butt. 'Stamp it out, this abominable evil of using children for pornography.' *Times* (London, 24 November 1977) accessed 28 February 2015 and J. Harrison, Political Reporter, 'Child Porn: Action at Last.' *Daily Mail* (London, 11 February 1978) accessed 12 February 2015.
[273] P. Symon, 'Fears over children lured into pornography.' *Times* (London, 9 February 1978) accessed 28 February 2015.

understandable given that the mass-production of devices capable of creating digital images was not witnessed until the 1980's[274]. This is demonstrated by the case of Tony Zalewski, a member of the 'Paedophile Information Exchange' who was arrested for importing magazines containing IDCSA in 1984[275]. However two years later, cases of IDCSA on video media were beginning to be reported[276] and in 1986, reports of computer usage for paedophile activity were beginning to be highlighted[277]. Yet despite these reports, it was not until 1994 with the Criminal Justice and Public Order Act 1994 (discussed in Section 3.5) that this form of image was considered, suggesting that the law was slow to respond to this form of technology.

3.3.4 Defences Under the PCA78

In introducing offences under the PCA78, concerns were raised regarding the prosecution of those who came in contact with IDCSA unintentionally[278]. In addition, fears that parents innocently photographing their children would become liable of subject to blackmail for their actions[279]. As a result, the PCA78 also introduced the following two statutory defences under Section 1(4).

> (a) that he had a legitimate reason for distributing or showing the photographs or (as the case may be) having them in his possession ; or
>
> (b) that he had not himself seen the photographs and did not know, nor had any cause to suspect, them to be indecent.

Although the PCA78 does not define what would constitute a legitimate reason, Parliamentary discussions indicate that IDCSA used for scientific research, as part of law enforcement or trial proceedings and even forms of aversion therapy for offenders may have been permitted[280]. It must be noted that the above defences are only available to those charged with an offence under sections 1(1)(b) and 1(1)(c) of the PCA78, there were no defences available to those charged with the offence of taking or publication. Further,

---

[274] E. P. Doherty, *Digital Forensics for Handheld Devices* (1st, CRC Press 2012) 41

275 Anon, 'PIE member faces child pornography charge.' *Times* (London, 17 November 1984) accessed 21 February 2015.

[276] Anon 'Child porn nurse sent to jail.' *Daily Mail* (London, 21 August 1986) accessed 21 February 2015.

[277] S. Tendler, Crime Reporter, 'Computer link used in child pornography.' *Times* (London, 29 July 1987) accessed 21 February 2015.

[278] A. A. Gillespie, 'Child pornography: balancing substantive and evidential law to safeguard children effectively from abuse' (2005) 9.1 International Journal of Evidence & Proof 29, 49

[279] I. H. Mills, 'Effects of child pornography.' *Times* (London, 15 February 1978) accessed 21 February 2015.

[280] HC Deb 14 July 1978, Vol 953, col 1919-848

there is limited discussion around the concern of parents taking photos of their own children.

Although retrospectively numerous issues regarding the PCA78 can be highlighted, they are as a result of significant developments in computing technology witnessed over the following 35 years. The PCA78 provided a foundation from which regulation of IDCSA could be built, whilst highlighting the UK Government's intention to outlaw this material. Yet despite the need to prosecute those involved in IDCSA, only 41 convictions were secured for the period up until the end of 1982 from its enactment[281]. Further, reports highlighted that although literature describing child abuse was available in abundance, it was rare to encounter IDCSA, with acts of child sexual abuse for the purpose of producing illegal imagery reported to be limited[282]. Further, MP John Brynmor suggested that the availability of IDCSA was restricted to those who were involved in child sex abuse and knew where to look for it[283]. Yet fears also existed that children were being lured into pornography[284], with the PCA78 seen as a method of supressing this.

The PCA78 marked the beginning of the legislative fight against IDCSA, despite a lack of clarity regarding the motivations for implementing it. Mixed Government response meant that the threat of IDCSA was not clearly defined and often, competing opinions regarding the need to regulate IDCSA were often expressed. Never the less, the PCA78 provided a starting point for the prohibition of IDCSA, and some 10 years later, with the CJA88, the next significant step was witnessed.

3.4 The Criminal Justice Act 1988

Following the enactment of the CJA88, Section 160 provided that 'it is an offence for a person to have any indecent photograph of a child (meaning in this section a person under the age of 16) in his possession'.

In 1984 and 1985, Geoffrey Dickens MP[285] proposed the need to prohibit the possession of IDCSA, suggesting access to it would encourage offenders to sexually abuse children. Despite such comments it was a further three years (and ten years after the PCA78), till the

[281] HL Deb 15 May 1984 vol 451 c1397WA
[282] Anon 'Bill to control child pornography makes the law more effective.' *Times* (London, 6 May 1978) accessed 12 February 2015.
[283] HC Deb 14 July 1978, Vol 953, col 1919-848 at 1847
[284] P. Symon, 'Fears over children lured into pornography.' *Times* (London, 9 February 1978) accessed 28 February 2015.
[285] HC Deb 27 June 1984 vol 62 cc1014-6 and HC Deb 29 November 1985 vol 87, col 1117-718

Government opted to legislate in order to extend the range of offices surrounding IDCSA by enacting the CJA88. An apparent problem with the PCA78 lay with its omission to make what is termed as 'private possession' an offence, sentiments echoed by Millwood and Livingston who suggested those who possess IDCSA drive the demand for it and ultimately increase acts of child abuse[286]. Despite statistics highlighted by Ferrers[287] directly prior to the CJA88's enactment showing limited prosecutions being brought under the PCA78 (significantly less than for acts of child sexual abuse[288]), the enactment of a possession offence was seen as necessary to completely supress the trade of IDCSA. Comments from the then Home Secretary Douglas Hurd indicated that a possession offence would allow law enforcement to prosecute individuals involved in underground paedophile groups, where proving distribution or taking may be difficult but possession easier to establish[289]. In doing so it prevented those who produce and distribute IDCSA from claiming that the material in their possession was solely for private use, a gap in law raising concerns[290].

Private possession describes those who maintain IDCSA for their own personal use, for only them to view or those who possess IDCSA with intent to show or distribute but it cannot be proven. Retrospectively, this was a significant oversight of the PCA78, first, arguably due to the fact that at the time of publication, research surrounding IDCSA was limited (and arguably remains so today) and the offence itself was only beginning to carry the stigma and media attention that it currently does (as identified in Chapter 1). Second, the connection between possession of IDCSA and further child offending was not strongly established, yet concerns regarding the links were increasing[291]. Finally, technology at this time did not offer the ability to make, access and distribute IDCSA on the scale that is now seen. This is despite reports from the Met police commissioner's report[292] indicating that an increasing use of video recording devices and associated copying facilities were leading to more IDCSA in circulation, driving concerns. Arguably at this point, possessors of IDCSA were limited to small pockets of individuals, typically those who could afford to engage in purchasing the material. However, the enactment of the CJA88 was not without concern, with Lord Monson

[286] A. Millwood Hargrave & S. Livingstone, *Harm and Offence in Media Content: A Review of the Evidence* (2nd, Intellect Books 2009) 115
[287] HL Deb 17 March 1988 vol 494 cc1251-3
[288] HC Deb 22 December 1988 vol 144 cc426-7W
[289] N. Wood, Political Correspondent, 'Labour backs Hurd on child pornography.' *Times* (London, 17 October 1987) accessed 21 February 2015.
[290] HC Deb 28 June 1988 vol 136, col 177-344
[291] HC Deb 27 June 1984 vol 62 cc1014-6. And; HC Deb 29 November 1985 vol 87, col 1117-718
[292] 1987/88 Cm 389 Report of the Commissioner of Police of the Metropolis for the year 1987 at 29

indicating that prohibiting access to IDCSA may lead to individuals seeking actual children to abuse, a worry that still exists today[293].

Wells *et al*.,[294] suggested "child pornography *possessors* may use child pornography to validate their sexual interest in children". Possession of IDCSA is the newest addition to the category of offences in English law surrounding IDCSA despite being over 25 years old. For almost ten years, the only punishable acts were creation, distribution and publication. Despite, as previously discussed, the links between possessing material and proceeding to sexually abuse children not being empirically proven, the risk of encouraging such behaviour was arguably a factor that contributed to the introduction of the legislation. The increasing amounts of IDCSA becoming available, coupled with the ease in which it could be accessed are also likely to have caused concern. Yet fundamentally, public awareness and subsequent disgust of IDCSA is the probable trigger for Government action.

3.4.1 Defences Under the CJA88

In light of the enactment of possession of IDCSA legislation, anxiety was increasing about the penalty for innocently stumbling across illicit material[295]. The CJA88 also introduced the following three defences under section 160(2) of the Act, available to those charged with an offence of possession in addition to those introduced in the PCA78.

> Where a person is charged with an offence under subsection (1) above, it shall be a defence for him to prove—
>
> (a)that he had a legitimate reason for having the photograph in his possession; or
>
> (b) that he had not himself seen the photograph and did not know, nor had any cause to suspect, it to be indecent; or
>
> (c) that the photograph was sent to him without any prior request made by him or on his behalf and that he did not keep it for an unreasonable time.

Defences 1(a) and 1(b) CJA88 mimic those defined previously under the PCA78. In addition, 1(c) CJA88 allows those who acquire IDCSA, albeit not intentionally (no request for it) to part possession with the images and ultimately preventing a possession prosecution. This

[293] HL Deb 22 July 1988 vol, 499 col, 1583-1710 at 1674

[294] M. Wells, D. Finkelhor, J. Wolak & K. J. Mitchell 'Defining Child Pornography: Law Enforcement Dilemmas in Investigations of Internet Child Pornography Possession' (2007) 8.3 Police Practice and Research 269

[295] HL Deb 22 July 1988 vol, 499 col, 1583-1710 at 1670 and S. Easton, 'Criminalising the Possession of Extreme Pornography: Sword or Shield?' (2011) 75 JCL 391

defence recognises that possession may not occur through deliberate acts, and provides individuals with a way of protecting themselves in such circumstances. Although this additional defence may seem logical, there remains ambiguity around what constitutes an unreasonable time, as it is not defined in statute, with this point elaborated on in Chapter 5.

The offence of possession when enacted was considered the least severe when compared to the other IDCSA offences, reflected by section 160(3) of the Act, where those found guilty were liable to a fine not exceeding level 5 on the standard scale, where offences under the PCA78 carry a custodial sentence.

Comments surrounding the motivation regarding the implementation of statutory defences to the possession offence at the time of legislating are limited. However retrospectively, the Home Office[296] made it clear that in enacting the CJA88 it did not aim to punish anyone who stumbled upon material or received it without consent. This sentiment was reiterated in *Collier*[297] where the court stated that it would not be correct to prosecute a person who was unaware of and had not seen the illegal material. As Marin[298] highlights, it was (although less likely than today through the use of the Internet) possible for those seeking adult pornography to find IDCSA through purely accidental means.

3.5 Criminal Justice and Public Order Act 1994

In the early 1990s the realisation of the number of child abusers in existence was beginning to dawn, with estimates in 1991 placing numbers at 2 million in the US and Canada with concerns raised about the methods they used to access IDCSA[299]. When enacted, the Criminal Justice and Public Order Act 1994 (CJPO94), section 84 was designed to 'future proof legislation'[300] surrounding IDCSA, providing a crucial stage in the UK Government's recognition of society's migration to computing technology, with increasing reports of computing technology used to access IDCSA[301]. The 1990's witnessed the commercialisation

[296] Home Office and Scottish Executive, 'Consultation: On the Possession of Extreme Pornographic Material' (2005) 1

[297] *Collier (Edward John)* [2004] EWCA Crim 1411

[298] G. Marin, 'Possession of Child Pornography: Should you be Convicted When the Computer Cache Does the Saving for You' (2008) 60 Fla. L. Rev. 1207

[299] L. S. Smith, 'Private Possession of Child Pornography: Narrowing at-Home Privacy Rights' [1991] Ann. Surv. Am. L. 1011, 1013

[300] 1993/94 HC 126 Home Affairs Committee. First report. Computer pornography at 67

[301] K. Alderson, 'Businessman, 48, collected child porn from Internet.' *Times* (London, 27 October 1995) accessed 12 February 2015 and P. Wilkinson & R. Gledhill, 'Paedophile priest circulated porn on the Internet.' *Times* (London, 13 November 1996) accessed 12 February 2015) and Anon, 'Gary Glitter 'in child porn probe'.' *Times* (London, 19 November 1997) accessed 12 Feb. 2015.

of the Internet and the increased affordability of computing and digital technologies[302]. In turn, the creation and transmission of digital files was becoming more frequent and publicised as communication protocols such as email were increasing in popularity. As a result, computing technology and the Internet were often highlighted as portals to a repository of IDCSA[303]. Further, as Foreman[304] comments, the use of camera and printing devices were increasing the ability for paedophiles to produce and mass distribute imagery. In turn, scanning devices in conjunction with computer graphics packages allowed a user to produce basic digital imagery[305].

In 1994, computing devices were identified as a tool that could be used to view and acquire IDCSA[306]. Yet the use of computing technology had however been recognised as a device for supporting paedophile activity some eight years prior to the enactment of the CJPO94 by Chock[307], not for the distribution of images, but as a means of communication between likeminded individuals. In addition, Conley[308] and Gilbert[309] raised concerns regarding computer usage to display advertisements for children to be involved in pornography, with reports of arrests for those who were running bulletin-board systems hosting such hoardings[310]. In order to tackle these technological developments, Section 84 CJPO94 provides the key incremental developments in IDCSA legislation raising the following four points of discussion.

The first addition made by the CJPO94 under section 84(2)(a)(i) was to amend Section 1(1)(a) of the PCA78 to include the phrase "to make" in the offence of taking. In doing so, the CJPO94 recognised the flexibility of digital data and the ease in which it can be created, edited and duplicated. No longer do offenders need to be at the scene of the child abuse

[302] D. B. Johnson, 'Why the Possession of Computer-Generated Child Pornography Can Be Constitutionally Prohibited' (1994) 4 Alb. L.J. Sci. & Tech. 311, 312

[303] P. Rose, Peter, Chief Crime Correspondent, '100 held in global child-porn swoop.' *Daily Mail* (London, 3 September 1998) accessed 21 February 2015) and L. Lee-Potter, 'Depravity on the Internet.' *Daily Mail* (London, 4 September 1998) accessed 21 February 2015

[304] J. Foreman, 'Can We End the Shame?--Recent Multilateral Efforts to Address the World Child Pornography Market' (1990) 23 Vand. J. Transnat'l L. 435, 438

[305] D. B. Johnson, 'Why the Possession of Computer-Generated Child Pornography Can Be Constitutionally Prohibited' (1994) 4 Alb. L.J. Sci. & Tech. 311, 312

[306] J. C. Scheller, 'PC Peep Show: Computers, Privacy, and Child Pornography' (1994) 27 J. Marshall L. Rev. 989, 989

[307] P. N. Chock, 'The Use of Computers in the Sexual Exploitation of Children and Child Pornography' (1987) 7.3 Computer/L.J. 383, 392

[308] P. C. Conley, 'Behind Closed Doors-The Clandestine Problem of Child Pornography.' (1987) 21 Creighton L. Rev. 917

[309] J. Gilbert, 'Computer bulletin board operator liability for user misuse.' (1985) 54 Fordham L. Rev. 439

[310] R. Manning, 'Plugging in to Computer Bulletin Boards.' (1986) ERIC Digest

taking photos to be guilty of the offence, but those who make new images from existing content are liable.

Traditionally IDCSA took the form of photos, magazines, and physical videocassettes[311]. However, the second addition of the CJPO94 under section 84 was to amend both the PCA78 and the CJA88 to recognise that "data stored on a computer disc or by other electronic means which is capable of conversion into a photograph". As electronic digital code stored on forms of digital storage media constituted a permanent record from which an image could be reproduced, the argument that digital data could constitute a photo was proposed[312]. This issue was highlighted in the subsequent case *Fellows*[313] in 1997, portrayed in the media as the first case of computer abuse of this kind[314]. The facts of the case are as follows. The defendant acquired an archive of approximately 11650 IDCSA, which had been manually categorised on the defendant's computer into a number of folders with descriptive names. The defendant contested his conviction suggesting that the storage of pictures on his hard disk drive did not constitute an offence under PCA78 section 1. In dismissing the defendant's appeal, it was held that electronic data held on digital storage media could constitute a copy of a picture. Particular reference was made to *Attorney General's Reference (No.5 of 1980)*[315], which stated that the OPA59 was wide enough to encompass videocassettes as articles capable of publication. In recognising this emerging technology and its potential role in IDCSA, it was held in *Fellows*[316] that the Government must have envisaged the PCA78 covering such devices as hard disk drives, despite not comprehending their usage when the Act was passed. In *Fellows*[317], a purposive approach was adopted to ensure that digital media could be brought within the confines of the PCA78 and CJA88, enabling legislation to regulate the material it was designed for. Further, the Home Affairs Committee[318] raised concerns that digital photographs were capable of bring printed, displayed on computer monitors and subject to electronic distribution via the Internet or transferable media like CDs, potentially increasing the prevalence of IDCSA, and providing further justification for prohibiting it. Therefore possession legislation was needed in order

[311] I. O'Donnell & C. Miller, *Child Pornography; Crime, computers and society* (1st, Willan Publishing 2007)
[312] 1993/94 HC 126 Home Affairs Committee. First report. Computer pornography. At 17
[313] *R. v. Fellows and Arnold* [1997] 1 Cr. App. R. 244
[314] C. Midgley. 'Employee 'kept porn library on university computer' *Times* (London, 30 March 1996) accessed 1 March 2015.
[315] *Attorney General's Reference (No.5 of 1980), Re* [1981] 1 W.L.R. 88
[316] *R. v. Fellows and Arnold* [1997] 1 Cr. App. R. 244
[317] *R. v. Fellows and Arnold* [1997] 1 Cr. App. R. 244
[318] 1993/94 HC 126 Home Affairs Committee. First report. Computer pornography. At 53

to tackle the rising volume of IDCSA in circulation and potentially preventing it from staying in circulation for longer due to people possessing it.

The third addition of the CJPO94 was to amend the OPA, to identify that 'data stored and transmitted electronically' could constitute publication[319], taking account of the Internet and the facilities it offers echoing the sentiment, "what is illegal offline is also illegal online"[320]. Rowbottom highlighted that the OPA and its provisions were significantly flawed when considered in the context of the Internet and that most obscene material was published from outside the jurisdiction of the UK, yet was still easily accessible by people within it[321]. Despite the fact that the act of downloading material could constitute publication[322], material could easily be acquired from abroad, clearly indicating a need to enact a possession offence. Often obscene material was created, hosted and distributed from countries with ineffective legal systems for policing this material[323].

The final key addition of the CJPO94 under section 84 is the recognition of a 'pseudo-photograph'. In 1993, the Home Affairs Committee[324] recognised the problems posed by images that had been manipulated to look like IDCSA under current legislation, relying on the material failing the test of obscenity in order to prosecute the publishers of this material. Such images included depictions of adults to look like children, or the addition of a child's head, superimposed onto an adult's body whilst engaging in sexual acts or posing[325].

The CJPO94 also provides interpretive guidance stating

> "Pseudo-photograph" means an image, whether made by computer-graphics or otherwise howsoever, which appears to be a photograph.
>
> If the impression conveyed by a pseudo-photograph is that the person shown is a child, the pseudo-photograph shall be treated for all purposes of this Act as showing a child and so shall a pseudo-photograph where the predominant impression conveyed is that the person shown is a child notwithstanding that some of the physical characteristics shown are those of an adult.

[319] L. Edwards & C. Waelde, *Law and the Internet* (3rd, Hart Publishing 2009) 632
[320] A. Travis, *Bound & Gagged: a Secret History of Obscenity in Britain* (1st, Profile Books 2000) 293
[321] J. Rowbottom, 'Obscenity laws and the internet: targeting the supply and demand' [2006] Crim. L.R. 97, 99
[322] *R. v Perrin* [2002] EWCA Crim. 747.
[323] A. Nair & J. Griffin, 'The regulation of online extreme pornography: purposive teleology (in)action' (2013) 21.4 Int J Law Info Tech 329
[324] 1993/94 HC 126 Home Affairs Committee. First report. Computer pornography. At 17
[325] 1993/94 HC 126 Home Affairs Committee. First report. Computer pornography. At 26

References to an indecent pseudo-photograph include—
a copy of an indecent pseudo-photograph; and

data stored on a computer disc or by other electronic means which is capable of conversion into a pseudo-photograph.

The above guidance stands to widen the net in relation to IDCSA, where focus is maintained on the content conveyed in the image itself. As a result, it is not just real photos of IDCSA that were prohibited, but images which were designed to depict acts of child sexual abuse.

As Manchester[326] stated, the effect of the CJPO94 was to remedy loopholes in existing legislation created by technological developments. The inclusion of legislation prohibiting pseudo-imagery prevented morphed images from falling outside of the range of offences in operation[327]. Given the existence of many complex computer-generated graphics packages capable of creating photographic representations, failure to patrol pseudo-photographs would leave a gap in the law for those capable of creating their own imagery using computer technology and distributing it. Although arguments existed that prohibiting pseudo-imagery amounted to a victimless crime as no depicted child is actually subject to sexual abuse, it was countered by concerns of harm caused to the child who is aware of being depicted as being abused[328]. Further, such material was seen as a harm to society with Stone[329] indicating that a main justification for prohibition of this material was to prevent it from being used to lure children into acts of child abuse for the production of new IDCSA.

The effects of the amendments introduced by the CJPO94 are wide ranging. First, a picture that has been spliced together to construe an image, which was not originally IDCSA but made to imitate such content, is sufficient to enable prosecution. Second, computer generated images appearing to be a photograph can now constitute IDCSA, providing they convey the impression that the individual depicted is a child. This is a particularly important expansion in the legislation as although possibly not envisaged at the time, software developments have subsequently made imagine generation and manipulation significantly easier[330]. Although not prevalent at the time of enactment, Photoshop artists trained in the

[326] C. Manchester, 'Criminal Justice and Public Order Act 1994: obscenity, pornography and videos' [1995] C. L. R. 123, 123
[327] D. Oswell, 'The Place of 'Childhood' in Internet Content Regulation A Case Study of Policy in the UK' (1998) 1.2 International Journal of Cultural Studies 271, 271
[328] 1993/94 HC 126 Home Affairs Committee. First report. Computer pornography. At 35-36
[329] R. Stone, 'Extending the Labyrinth: Part VII of the Criminal Justice and Public Order Act 1994.' (1995) 58.3 The Modern Law Review 389
[330] M. Fineman, *Faking it: Manipulated Photography Before Photoshop* (1st, Metropolitan Museum of Art 2012)

use of software such as Adobe Photoshop[331] can now produce pornographic images without reference to actual real life people. Although not a significant issue in 1994, now IDCSA can be produced which depicts no actual real world victim where realistic depictions of children can be made without a child being involved[332].

It is difficult to assess the impact of the CJPO94 in terms of convictions. However prosecutions under the PCA78 between 1996-1998 totalled 254 and 265 under the PCA88[333]. The CJPO94 also facilitated a number of high-profile prosecutions, including that of Gary Glitter, when staff at PC World identified digital IDCSA on his computer[334], and the Chancellor Kenneth Clarke's advisor Peter Hayden through the recognition of digital IDCSA[335].

Although digital data constituting a photograph was now recognised, the functionality and means of acquiring this data was still to be discussed. As the Internet continued to increase in prevalence, its usage as a portal to IDCSA became apparent. When a website providing access to IDCSA is visited, offenders can acquire this material on their device by a process of intentionally downloading. However, clarification was needed as to whether the act of downloading IDCSA by an offender would constitute an act of 'making' under Section 1 PCA78, one of possession or whether this act would fall outside of the boundaries of the law. This issue was addressed in Bowden[336].

3.6 1999 - *R v Bowden*

In 1999, the case of *Bowden*[337] provided clarification regarding the physical duplication of IDCSA and downloading of IDCSA from the Internet. The appellant submitted a computing device for repair to a local firm, from which indecent material was discovered. Upon examination, it was revealed that numerous IDCSA had been downloaded from the Internet and stored on the appellant's digital storage media.

---

[331] Adobe, 'Photoshop CC' (www.adobe.com 2013) <http://www.adobe.com/uk/products/photoshop.html> accessed 19 December 2013

[332] A. A. Gillespie, 'Defining Child Pornography: Challenges for the Law' (2010) 22 Child & Fam. L. Q. 211

[333] HC Deb 08 December 1999 vol 340 c533W

[334] Anon, 'Gary Glitter 'in child porn probe'' *Times* (London, 19 November 1997) accessed 27 February 2015

[335] A. Lee, 'Child pornography videos found at home of Chancellor's adviser.' *Times* (London, 14 January 1997) accessed 27 Feb. 2015.

[336] *R v Jonathan Bowden* [2000] 1 Cr. App. R. 438

[337] *R v Jonathan Bowden* [2000] 1 Cr. App. R. 438

In the case of *Bowden*[338], three key issues were resolved. First, it confirmed that those involved in the creation of pseudo-photographs under Section 1(1)(a) PCA78 did not have to have contact with the subjects of the images in order to be prosecuted[339]. In doing so, the courts recognised that the offence of taking (and amended to include 'making') was not only an offence that could be committed by those in direct contact with children, but by those with access to the necessary technology to create IDCSA from existing content. Second, downloading an IDCSA constituted an act of making under the PCA78 section 1(1)(a)[340]. Finally, making a copy of an IDCSA could also constitute a making offence[341]. The second and third points are of upmost importance to developments in the offence under Section 1(1) PCA78 as the statute omits to define what constitutes an act of making. Similarly, this ruling demonstrated a response to the changing landscape of IDCSA and the more prominent use of computer technology to access it. Further it allowed the legal system to more effectively tackle those who were making IDCSA.

In recognising the emergence of the Internet and the prevalence of IDCSA hosted online now meant that those interacting with this content online could be subject to offences under the PCA78. Lord Justice Otton[342] stated that 'we find it impossible to conclude that the reproduction of indecent material to be found on the Internet was not within the mischief aimed at by the legislation when the words "to make" were included in the amending statute'. Further, at this point, there is still no available statutory defence for those liable under section 1(1)(a) PCA78, despite the extended scope of the Act, leaving law enforcement and those who investigate crimes of IDCSA vulnerable to prosecution[343]. Often, to effectively investigate IDCSA offences, law enforcement practitioners have to extract content from digital devices for analysis. This very act creates a duplicate of any IDCSA present on a device, ultimately an act of making within the scope of law at the time. Yet this act is done with the intention of supporting the criminal justice system and their investigation.

[338] *R v Jonathan Bowden* [2000] 1 Cr. App. R. 438
[339] *R v Jonathan Bowden* [2000] 1 Cr. App. R. 438 at 443
[340] *R v Jonathan Bowden* [2000] 1 Cr. App. R. 438 at 438
[341] *R v Jonathan Bowden* [2000] 1 Cr. App. R. 438 at 443
[342] *R v Jonathan Bowden* [2000] 1 Cr. App. R. 438 at 445
[343] IWF, 'R V Bowden' (*iwf.org,* n.d.) <https://www.iwf.org.uk/hotline/case-laws/r-v-bowden> accessed 10 January 2015

Inevitably, in dealing with the Internet in *Bowden*[344], the true intricacies of computer systems were beginning to be revealed. As a result, simple possession of IDCSA in this environment was a complex legal challenge with a precedent yet to be set. Particularly, as individuals browsed the Internet, the content they were viewing would be stored in their device's Internet Cache. If an individual browsed websites hosting IDCSA, often a copy of these images would be stored in this cache. The question remained as to whether this content was possessed by an individual. This was to be addressed in *Atkins*[345].

3.6.1 2000 - *DPP v Atkins*

In 2000, the case of *Atkins*[346] provided the first clarification surrounding the offence of possession under the CJA88. It was held that unless the defendant knew that they had the photographs in his possession he couldn't be prosecuted under Section 160 CJA88, making knowledge a requisite for the offence[347]. As the IDCSA in question in *Atkins*[348] were stored within the Internet cache on the appellant's computer system (further discussion of the cache is included in Chapter 5), knowledge of the cache and files it contained was deemed necessary. Therefore those who were not aware of how the Internet cache worked or in turn, that it even existed, following this ruling could not be in possession of files residing in there. In addition, the offences under section 1(1)(a) PCA78 were extended, where '"making" includes copying photographs providing that it is done knowingly'[349], further acknowledging the prevalence of digital data and its ease of duplication. The inclusion of an element of 'knowingly' means that images that are duplicated via automated processes unknown to an individual (for example, via hidden computer system processes) are unlikely to be categorised as an act of making. The final point to take from *Atkins*[350] was the court consideration of a defence of 'legitimate reason' for possessing IDCSA, from which it was ruled that the validity of which 'is a simple question of fact (for the magistrate or jury) in each case' to determine[351].

In addition to *Atkins*[352], the turn of the millennium also witnessed the enactment of the *Criminal Justice and Court Services Act 2000* and its review of punishments for IDCSA

[344] *R v Jonathan Bowden* [2000] 1 Cr. App. R. 438
[345] *Atkins v Director of Public Prosecutions* [2000] 2 Cr. App. R. 248
[346] *Atkins v Director of Public Prosecutions* [2000] 2 Cr. App. R. 248
[347] *Atkins v Director of Public Prosecutions* [2000] 2 Cr. App. R. 248, at 249
[348] *Atkins v Director of Public Prosecutions* [2000] 2 Cr. App. R. 248
[349] *Atkins v Director of Public Prosecutions* [2000] 2 Cr. App. R. 248, at 249
[350] *Atkins v Director of Public Prosecutions* [2000] 2 Cr. App. R. 248
[351] *Atkins v Director of Public Prosecutions* [2000] 2 Cr. App. R. 248 at 262
[352] *Atkins v Director of Public Prosecutions* [2000] 2 Cr. App. R. 248

offences. In the late 1990's media attention began to focus on penalties associated with those prosecuted, particularly on the severity and perceived lack of[353]. The UK government acknowledged increasing public concern[354] and chose to act.

3.6.2 Criminal Justice and Court Services Act 2000

The Criminal Justice and Court Services Act 2000 continued the recognition in English law of the severity of IDCSA offences, implementing stronger punishments for those guilty of offences in this area. Gillespie[355] suggests that the strength of society's condemnation of child abuse and associated acts has trigged the need for severe punishments. However, it is arguable that the increasing amount of IDCSA in circulation warranted stronger punishments to act as a deterrent with Williams[356] stating that IDCSA was now easily accessible and free to acquire. Under section 41 of the Act, the PCA78 was amended to increase the maximum punishment from three to 10 years' imprisonment. Further the CJA88 was amended to increase the maximum punishment from a fine not exceeding level 5 on the standard scale to five years imprisonment, reflecting views that it is the least severe of the IDCSA offences[357]. Increases in punishments also coincided with the Government's substantial investment in provisions capable of investigating those involved in IDCSA, including the implementation of the National Hi-Tech Crime Unit and incentives to support tracking IDCSA online[358].

3.6.3 2002 - *R v Smith & Jayson*

In 2002, the joint cases of *Smith & Jayson*[359] clarified the following two points of law in this area.

First in relation to Smith, the act of opening an email with an IDCSA attached was considered. Lord Justice Dyson acknowledged "electronic communication by means of the Internet and e-mails has led to an explosion in the dissemination of pornographic material,

[353] S. Heffer, 'Don't Let Them Slip the Net.' *Daily Mail* (London, 5 September 1998) accessed 2 March 2015.
[354] HL Deb 4 October 2000 vol 616, col 1509-1680 at 1551
[355] A. A. Gillespie, 'Child pornography: balancing substantive and evidential law to safeguard children effectively from abuse' (2005) 9.1 International Journal of Evidence & Proof 29, 49
[356] K. S. Williams, 'Child-Pornography and Regulation of the Internet in the United Kingdom: The Impact on Fundamental Rights and International Relations' (2002) 41 randeis L.J. 463, 469
[357] HL Deb 3 July 2000 vol 614, col 1275-1378
[358] HC Deb 18 December 2001 vol 377 cc251-2W
[359] *R v Graham Westgarth Smith, Mike Jayson* [2002] EWCA Crim 683

and in particular of indecent photographs of children"[360]. As a result, to fall within an offence of PCA78 section 1(1)(a), an offender must intentionally open up the email and attachment, knowing that it was or likely to be IDCSA. It is key to note that the surrounding circumstances of a case may be considered, and here, evidence of Smith engaging in communications with paedophilic content allowed inferences of knowledge to be inferred. This position was summarised by Lord Justice Dyson[361].

> 'a person simply opening an unsolicited e-mail message and opening the attachments to it in ignorance of their actual or likely contents, we would have no difficulty in holding that the facts did not disclose an offence of making, contrary to section 1(1)(a) of the 1978 Act, or indeed of being in possession contrary to section 160(1) of the 1988 Act'.

Second, in relation to *Jayson*[362], the act of downloading an image from the Internet constituted an act of 'making' providing there was evidence that the act was "deliberate and intentional act with knowledge that the image made is, or is likely to be an indecent photograph or pseudo-photograph of a child"[363]. This provided further clarity surrounding IDCSA found in the Internet cache in addition to *Atkins*[364]. Following *Jayson*[365], the challenges of establishing an individuals knowledge of the cache in order to establish possession are negated as if evidence of intentional searching online for IDCSA can be found, a making prosecution can be brought instead. In addition, there is no requirement for the offender to intend to store the images for the purpose of retrieving them in the future, and further, 'it is not a requirement that the data should be retrievable' and therefore accessible, a requirement for establishing possession[366].

3.7 The Sexual Offences Act 2003

As discussed in Chapter 2, one of the goals of legislation concerning IDCSA is to safeguard children from mistreatment and from the sustained dissemination of pictures depicting their exploitation. However, to establish what constitutes IDCSA, it is necessary to establish who is a child. The Sexual Offences Act 2003 section 45(2*)* extended the definition of a child to anyone under 18, an increase from the previous position of 16, following concerns that children remain vulnerable up until the age of 18 and to comply with the United Nations

[360] *R v Graham Westgarth Smith, Mike Jayson* [2002] EWCA Crim 683
[361] *R v Graham Westgarth Smith, Mike* Jayson [2002] EWCA Crim 683
[362] *R v Graham Westgarth Smith, Mike Jayson* [2002] EWCA Crim 683
[363] *R v Graham Westgarth Smith, Mike Jayson* [2002] EWCA Crim 683 at 34
[364] *Atkins v Director of Public Prosecutions* [2000] 2 Cr. App. R. 248
[365] *R v Graham Westgarth Smith, Mike Jayson* [2002] EWCA Crim 683
[366] *R v Graham Westgarth Smith, Mike Jayson* [2002] EWCA Crim 683 at 34

Convention on the Rights of the Child which defined a child as someone under 18[367]. Therefore the first criterion to consider when establishing IDCSA is that a photo or video depicts an individual who appears or is under this age of 18. This raises the first main issue regarding IDCSA. In many circumstances, the person(s) depicted in images are unknown to the offender and those involved in the prosecution. When establishing age, the previous case of *Land*[368] states it is for the jury to determine whether an image depicts a person under the age of 18, and is therefore illegal. There is no requirement for expert evidence on this matter. However, CEOP's ChildBase, a database of known illegal imagery, may provide some assistance when determining the legality of an image should an offender maintain images already contained within this database (images which are known from past cases to be deemed illegal).

The move to increase the legal age of a child to 18 also raised a number of addition concerns highlighted by the Home Affairs Committee[369] which are noted as follows. First, the issue of determining the age of a child would likely result in difficult judgement calls having to be made by law enforcement when determining if an image is illegal. Second, as the age of sexual consent was 16, there is a grey area where individuals can engage in sex but not be depicted. Third, worries were expressed that magazines aimed at the teenage market depicting provocative images may fall foul of the new child threshold. Finally, it was perceived as a better use of police resources to tackle those with images depicting grave acts with obviously underage children. As there is limited comment on this final point, one can only presume that this may be due to a supposition that harm to younger children may be greater and the potential to waste resources investigating images which may turn out to be individuals who are aged 18 or over but look younger.

Influenced by the ruling in *Bowden*[370] and the fact that creating a copy of an IDCSA now constituted making[371], the Sexual Offences Act 2003 also introduced the first defences to the offence under PCA78 section 1(1)(a). Section 46(1) of the Sexual Offences Act 2003, permits the making of IDCSA if it is in the interest of crime detection and prevention by UK bodies.

[367] HL Deb 04 October 2000 vol 616 cc1564-89. And; United Nations Convention on the Rights of the Child, Article 1
[368] *R v Land* [1998] 1 Cr App R 301
[369] 2002/03 HC 639 House of Commons. Home Affairs Committee. Sexual Offences Bill at 79
[370] *R v Jonathan Bowden* [2000] 1 Cr. App. R. 438
[371] IWF, 'R V Bowden' (*iwf.org,* n.d.) <https://www.iwf.org.uk/hotline/case-laws/r-v-bowden> accessed 10 January 2015

Following the enactment of the Sexual Offences Act 2003, it was a further three years before the next significant development in IDCSA law was witnessed, with the courts forced to tackle the concept of possession once again, but in relation to deleted content.

3.8 2006 - *R v Porter*

Although the CJA88 enacted an offence of possession it omitted to provide a statutory definition of what actually constituted possession. Although this appears to be a significant oversight, possession is a long established concept in law, particularly in reference to tangible chattels. As noted in Chapter 1, IDCSA at the time of this legislation was predominantly in books, magazines or videocassettes, all tangible objects, allowing existing legal tests of possession to be applied in cases. However, as witnessed by the CJPO94, some six years later, the UK Government acknowledged the emerging importance of digital data and computing technology. Even at this point, the intricacies of and difficulties posed by possessing intangible digital content were not addressed.

In 2006, the case of *Porter*[372] directly addressed what constituted possession of digital IDCSA on a digital device or computer system (an in-depth discussion of *Porter*[373] is provided in Chapter 4) and sought to provide clarification on whether deleted files can be possessed. Traditionally, possession requires knowledge of and custody and control over the item in question, in order for a person to be in possession of it (see *Boyesen*[374] for further expansion). *Porter*[375] confirmed that this test should remain and therefore to be in possession of a digital IDCSA, the offender must have knowledge of its existence and be able to access it, therefore having custody and control of it, a fact for the jury to determine given the circumstances of the case. Notably, *Porter*[376] set a precedent for dealing with deleted IDCSA, confirming that they could not be possessed unless the offender had the ability to re-access them (through specialist software) at the time of arrest for the offence.

The decision in *Porter*[377] provided an attempt to address the complexities of computer systems when used in conjunction with possessing IDCSA. Yet such complexities had not subsided, with prosecution being subject to levels of computer literacy and the difficulty in assessing a defendant's level of computer literacy in order to determine possession, which

[372] *Porter* [2006] 2 Cr. App. R. 25
[373] *Porter* [2006] 2 Cr. App. R. 25
[374] *R. v Boyesen* (1982) 75 Cr.App.R. 51, 53; [1982] A.C. 768
[375] *Porter* [2006] 2 Cr. App. R. 25
[376] *Porter* [2006] 2 Cr. App. R. 25
[377] *Porter* [2006] 2 Cr. App. R. 25

will be expanded upon in the remainder of this thesis. Further, the UK Government were preparing to create a new classification of IDCSA in English law, those termed 'prohibited images'[378].

3.9 Coroners and Justice Act 2009 – Prohibited Images

The final development in legislation surrounding IDCSA to be considered in this chapter is the introduction of the concept of a 'prohibited image'. Such images include cartoon pornography and drawings, described in *Palmer*[379] as "stylised fantasy images in graphic cartoon format". These images do not depict a real-world individual, but one that has been created via computer graphics programmes. A prohibited image also includes those that are a by-product of real IDCSA, such as tracings, items that were currently unregulated[380]. Although the technology to produce these type of images had been available long before this enactment, concerns were raised that this form of image were fuelling peoples desires to sexually abuse children[381]. In 2011, Steven Freeman, a former head of the Paedophile Information Exchange (PIE) was the first to be prosecuted under the act for possessing approximately 3000 drawings[382].

A prohibited image is distinguished from previous illegal forms of imagery and defined under CJA09 Section 62(2) as an image which is pornographic and grossly offensive, disgusting or otherwise of an obscene character and one which falls within Section 62(6) CJA09. Under Section CJA09 62(3), an image is pornographic "if it is of such a nature that it must reasonably be assumed to have been produced solely or principally for the purpose of sexual arousal". The test is objective, based on the standard of reasonableness when considering material for the purposes of sexual arousal. Section 62(6) CJA09 requires the image to focus solely or principally on a child's genitals or anal region. If the image does not maintain this focus but depicts an act under Section 62(7) CJA09 (for example, intercourse

---

[378] Home Office, *Consultation on Possession of Non-photographic Visual Depictions of Child Sexual Abuse* (Home Office, 2007) <http://www.scotland.gov.uk/Resource/Doc/1099/0048474.pdf> accessed 15 January 2016

[379] *R. v Palmer* [2011] EWCA Crim 1286

[380] A. Antoniou, 'Possession of prohibited images of children: three years on' (2013) 77.4 J. C. L. 337, 349

[381] Home Office, *Consultation on Possession of Non-photographic Visual Depictions of Child Sexual Abuse* (Home Office, 2007) <http://www.scotland.gov.uk/Resource/Doc/1099/0048474.pdf> accessed 15 January 2016

[382] Anon, 'Ex-paedophile group leader Freeman jailed over child rape drawings' *BBC News* (London, 15 July 2011) <http://www.bbc.co.uk/news/uk-england-london-14169406> accessed 16 January 2015 and IWF, 'R v Freeman' (iwf.org, n.d.) <https://www.iwf.org.uk/hotline/case-laws/r-v--freeman> accessed 16 January 2015

with an animal etc.), then the image is still classed as prohibited, where acts include the performance by a child of an act of intercourse with an animal.

The justification for regulating this material stems from a 'concern that such material reinforces inappropriate feelings towards children' [383]. However, this is arguably a controversial enactment due to a lack of definitive research showing correlations between viewing this form of material and a tendency to carry out sexual child abuse[384]. Antoniou[385] highlights that no research had been carried out at the time to definitively establish any dangerous correlations leading to suggestions that the offence is overbroad. However, concerns had been raised that prohibited images of children could be used as tools to groom victims[386].

Trepidations have been raised that offences under the CJA09 amount to a victimless crime with no one actually being hurt through pure thoughts alone[387]. In addition, Johnson and Rogers[388] suggested that virtual images may decrease the likelihood of actual cases of child abuse from occurring creating comparisons to the use of synthetic heroin for drug rehabilitation patients. However, arguments for regulating this material may lie with the supposed implicit link between those who view this form of material and those who want to engage in acts of actual sexual child abuse (discussed in Chapter 2).

The CJA09, section 64 implements three defences against possession of prohibited images, mimicking those seen under the CJA88 Section 160(2). Finally, custodial sentences of offences of possessing prohibited images of a child carrying a maximum of 3 years in accordance with CJA09 Section 66, recognising the offence as less severe than those of possession illegal IDCSA.

---

[383] Home Office, *Consultation on Possession of Non-photographic Visual Depictions of Child Sexual Abuse* (Home Office, 2007) <http://www.scotland.gov.uk/Resource/Doc/1099/0048474.pdf> accessed 15 January 2016

[384] Home Office, *Consultation on Possession of Non-photographic Visual Depictions of Child Sexual Abuse* (Home Office, 2007), 1 <http://www.scotland.gov.uk/Resource/Doc/1099/0048474.pdf> accessed 15 January 2016

[385] A. Antoniou, 'Possession of prohibited images of children: three years on' (2013) 77.4 J. C. L. 337, 349

[386] Home Office, *Consultation on Possession of Non-photographic Visual Depictions of Child Sexual Abuse* (Home Office, 2007), 6 <http://www.scotland.gov.uk/Resource/Doc/1099/0048474.pdf> accessed 15 January 2016

[387] Home Office, *Consultation on Possession of Non-photographic Visual Depictions of Child Sexual Abuse* (Home Office, 2007), 13 <http://www.scotland.gov.uk/Resource/Doc/1099/0048474.pdf> accessed 15 January 2016

[388] M. Johnson & K. M. Rogers, 'Too Far Down the Yellow Brick Road - Cyber-Hysteria and Virtual Porn' (2009) 4 J. Int'l Com. L. & Tech. 61, 61

3.10 Concluding Thoughts

This chapter has chronologically examined the existing law surrounding IDCSA offences, highlighting developments over the past 50 years, commencing with the OPA. Law in this area has been shaped by developments in technology, as new methods for creating, accessing and storing IDCSA are devised which can be seen with the amendments to existing legislation brought in by the CJPO94 and acknowledgment of cartoon imagery by the CJA09. In turn, the influence of media on society's waning tolerance for IDCSA must not be underestimated. It is arguable that law in this area has been slow to develop in regards to emerging technology, often failing to take a proactive stance, inevitably leading to periods of time where significant gaps in legislation are apparent. This can be seen in a number of instances, first with the initial omission to develop a possession offence in 1978, followed by a 6-year period between the PCA88 to the CJPO94 where developments in digital photographs were not formally recognised. Although the reasons behind these omissions have been discussed, it indicates that the law is primarily reactive to developments in this area.

At present, England and Wales maintains four foundation offences surrounding IDCSA, those of taking (or making), distribution, publishing and possession. However, the remainder of this thesis will maintain focus on possession alone. In principle, possession may appear to be a straightforward offence, however in practice, developments in technology have now created a complex and multifaceted area of law, posing a challenge to law enforcement. According to Crown Prosecution Service[389] figures, there have been on average around 4000 prosecutions for offences of possession per year since 2010, and the complexity of establishing possession now overlaps onto the offences in relation to extreme pornography. Establishing possession of IDCSA in many cases will now involve establishing whether data on a digital device is possessed, taking into accounts its intangible nature and the complexities of computer systems. Chapter 4 focuses on an analysis of the concept of possession, the current test of possession in IDCSA offences and its application.

[389] CPS, 'Violence against Women and Girls Crime Report' (2015) <http://www.cps.gov.uk/publications/docs/cps_vawg_report_2015_amended_september_2015_v2.pdf> accessed 30 November 2015

Chapter 4

A Focus on the Possession Offence

4.1 Introduction

In Chapter 3, the development of legislation surrounding offences of IDCSA was presented and analysed to provide background context to this area. Now, Chapter 4 will focus upon the offence of possession under section 160 CJA88 due to the difficulties posed by the current test of possession and its relevance in relation to technological developments.

To commence, the general legal concept of possession is discussed, providing an overview of legal definitions of possession across a range of offences including illicit substances and firearms to introduce this area. Attention is then turned to possession of IDCSA, the application of possession law in this area and the challenges faced by legal professionals. There is a fundamental change in the type of IDCSA that is now regularly possessed, often no longer a physical photograph or magazine but a digital representation contained within digital storage media on a digital device. The commercialisation of the Internet and the presumed anonymity that it provides has encouraged the mass distribution and creation of digital IDCSA. The principles behind enforcing a prohibition of possession are sound; through prohibiting possession it is argued that demand for the material will lessen, leading to limited production and fewer acts of child sexual abuse from which the material is created. Yet the task of regulating possession is now difficult, where law enforcement are left to patrol intangible digital data, which can be created and transferred between offenders in seconds and is stored upon complex devices. This change has led to numerous difficulties in applying tests of possession in the context of IDCSA due to the complexities of computer system architecture and associated devices.

To provide an underpinning knowledge of possession, this Chapter commences with a general discussion of the concept of possession to contextualise this area of law.

4.2 What is Possession?

Before delving into the complexities of possession in IDCSA cases, the linguistic definition of possession is presented. The Oxford Dictionary[390] defines possession as a "state of having, owning, or controlling something", a word frequently used to denote an individual's relationship with their chattels. At face value, possession appears to be an obvious conception, one that should be easy to apply in law, yet such sentiments are not universally shared. In *Boyesen*[391], a case surrounding illicit substance acquisition, possession was described as "a deceptively simple concept" and the underlying principles of applying it are often overlooked. Domestic statutes fail to provide interpretive assistance and Lord Scarman[392] suggests that in absences of a uniform definition, when considering possession thought must be given "to the term having regard to the mischief that the applicable legislation was designed to prevent".

Given these difficulties, in *Boyesen*[393], the following legal definition was produced; "possession denotes a physical control or custody of a thing plus knowledge that you have it in your custody or control"[394], stemming from Lord Wilberforce's comments in *Warner*[395] a case surrounding the possession of illegal substances. These elements consistently appear in cases of possession (see for example *Taylor*[396], *Deyemi*[397], *Adams*[398]) offences across English law and provide a starting point for discussions surrounding this area.

4.2.1 Types of Possession

The requirement to establish possession is a vital aspect of many offences within the legal domain in England and Wales. This section provides an overview of the application and development of possession in a range of offences, which ultimately the law surrounding the possession of IDCSA has taken on board in its application. Possession and its use can generally be categorised into two main areas.

---

[390] Oxford Dictionaries, 'Definition of possession in English ' (Oxford Dictionaries, 2013) <http://oxforddictionaries.com/definition/english/possession?q=possession> accessed 19 August 2013

[391] *R. v Boyesen* (1982) 75 Cr.App.R. 51, 53; [1982] A.C. 768

[392] *R. v Boyesen* [1982] A.C. 768; per Lord Scarman at 770

[393] *R. v Boyesen* (1982) 75 Cr.App.R. 51, 53; [1982] A.C. 768

[394] *R. v Boyesen* (1982) 75 Cr.App.R. 51, 53; [1982] A.C. 768

[395] *Reg. v. Warner* [1969] 2 A.C. 256

[396] *R. v Taylor (Lee Robert)* [2011] EWCA Crim 1646

[397] *R. v Deyemi* (Danny) [2007] EWCA Crim 2060

[398] *Adams v DPP* [2002] EWHC 438 (Admin)

Strict liability possession: In strict liability possession offences, possession is established when an offender is found to be in physical possession of the article (on the person or property, depending on the offence in question). There is no requisite mental element needed to be proven and in some circumstances, no need to prove knowledge of the item allegedly possessed (further analysis provided in section 4.2.2). Clough[399] identifies this as 'simple possession'. This is due to the chattel in its own right being something, which should never, under any circumstances, be possessed by a particular individual, demonstrated in cases of possession of prohibited weapons[400]. Here, legislation is concerned only with the type of item and its potential danger to society or individuals, prompting a less stringent threshold for the offence to be established.

Possession with intent: The second application of possession occurs when an offence requires the requisite intention regarding the item in question to be established. In this circumstance, possession arises when (despite the chattel in question not being a prohibited item or the item itself does not pose an initial hazard); the intention of the suspect is to use the item to cause harm. This is documented through possession offences under section 57 of the Terrorism Act 2000. Simple possession of the item is not enough and the offenders intended 'purpose connected with the commission, preparation or instigation of an act' must be established. Here, for example, the possession of certain paper-based documents may not in itself constitute an offence; however underlying motivation to use these documents might constitute a crime. For example, see *Rowe*[401], where possession of a notebook documenting instructions for creating and using a mortar was examined.

Both types of possession are applied throughout English law and a brief discussion of their application to various offences is required.

4.2.2 Possession in Different Offences

From *Boyesen*[402] it has been established that the elements of 'custody', 'control' and 'knowledge' are central to establishing possession however their application varies regarding different offences with the following providing a brief overview of their application.

[399] J. Clough, 'Now you see it, now you don't: digital images and the meaning of 'possession'' (2008) 19 Criminal Law Forum 205
[400] *R. v Deyemi (Danny)* [2007] EWCA Crim 2060
[401] *R. v Rowe (Andrew)* [2007] EWCA Crim 635
[402] *R. v Boyesen* (1982) 75 Cr.App.R. 51, 53; [1982] A.C. 768

In the context of possession of drugs, the Misuse of Drugs Act 1971 s28 states that for possession, a person must know they have the substance under their control. However, knowledge of the substance type is not required[403] and it is sufficient for an offender to know they are in possession of 'something'[404]. Roberts[405] argues that as most offenders will deny knowledge of a substance, it is necessary to place the burden of vetting their chattels prior to taking them into possession onto the individual. Control is established if the offender has knowledge of the item they possess or can exercise their power over the substance.

This can be contrasted with offences under the Terrorism Act 2000 s57 where the case of *R v G and J*[406] stated that under this section, a defendant must have knowledge of the item and control over it. In addition, the test of knowledge was extended where knowledge for this offence must include knowledge of the content of the item.

In cases of firearms possession, the basic requirements of possession are simply 'custody or control' where the offence is one of strict liability[407]. Fortson[408] states that Parliament has placed its focus on the nature of the item, which is being policed, and in some cases, chosen to omit the element of knowledge when establishing possession, due to the potential consequences that may stem from having the article in possession; therefore simply having the item is severe enough to constitute an offence.

The examples above provide a brief insight into the processes involved when attempting to establish possession. Low and Llewelyn highlight the difficulties involved in applying legal principles of possession and that such application can lead to complex and contentious debates, due in part to the diverse range of items, which can be subject to a claim for possession[409]. Additional discussion of the wider application of possession remains beyond

[403] P. Roberts, 'Drug dealing and the presumption of innocence: The Human Rights Act (almost) bites' (2002) 6.1 International Journal of Evidence & Proof 17, 23
[404] *R* v *McNamara* (1988) 87 Cr App R 246, CA.
[405] P. Roberts, 'Drug dealing and the presumption of innocence: The Human Rights Act (almost) bites' (2002) 6.1 International Journal of Evidence & Proof 17, 23
[406] *R v G and J* [2009] UKHL 13 at para 53
[407] *R. v Williams (Orette)* [2012] EWCA Crim 2162; [2013] 1 W.L.R. 1200 (CA (Crim Div))
[408] R. Fortson, 'R. v Williams (Orette): burden of proof - firearms offence' (2013) Crim. L.R. 983, 985
[409] K. F.K. Low & D. Llewelyn, 'Digital files as property in the New Zealand Supreme Court: innovation or confusion?' L.Q.R. 2016, 132(Jul), 394-399. See also the New Zealand case of *Dixon v Queen, The* [2015] NZSC 147 (Sup Ct (NZ)), involving the decision as to whether digital files can constitute property and therefore be possessed.

the scope of this thesis; therefore the following sections of Chapter 4 will focus on the main elements of a typical possession test before concentrating on the possession of digital files.

4.2.3 Summary of Possession Elements

What can be summarised from the above points is that typically possession currently has three elements, 'knowledge', 'custody' and 'control', of which the latter two cannot be inferred without knowledge of the article. Green[410] expands upon the latter element, stating that control has in itself two further components, direct control (a means of physical contact with the property) and indirect (a means of accessing the property). Bovey[411] further clarifies that when attempting to establish control, consideration must be given to the surrounding circumstances of the case as 'control is not a function of the unconscious' and evidence must be present to demonstrate this. These sentiments are echoed in the case of *McMurray*[412]. The alleged offence was one of possession of terrorist material, where it was indicated that possession must be voluntary, involving actual or potential physical control inferring that some form of positive act by the defendant is required to participate in possession with an article.

As each application of the definition of possession differs depending on the offence type, some ambiguity is caused. Shartel[413] describes the term 'possession' as a vague legal concept, difficult to define and apply consistently. This complexity is demonstrated in *Cheung*[414].

> Possession causes a lot of problems for juries, and for judges and lawyers generally. You might be in possession of something because somebody's slipped it into your pocket, but you wouldn't know it was there because somebody slipped it in without you being aware of it. You wouldn't have knowledge of it being in your possession. You can have possession of something, which you may not physically have in your control. You may have given it to someone else, but you actually possess it and can control it. There are many different ways of looking at possession.

From *Cheung*[415], it is apparent that the three elements of 'custody', 'control' and 'knowledge' can function independent of one another, and even when all three elements

[410] S. Green, 'The subject matter of conversion' (2010) J.B.L. 218, 221
[411] K. S. Bovey, 'Possession revisited' (2005) S.L.T. 475, 475
[412] *R v McMurray* [1996] 8BNIL n30
[413] B. Shartel, 'Meanings of Possession' (1932) 16 Minn. L. Rev. 611
[414] *R. v Ping Chen Cheung* [2009] EWCA Crim 2965 at 20
[415] *R. v Ping Chen Cheung* [2009] EWCA Crim 2965 at 20

are not present, possession may still seem apparent. This raises the main complexity in possession cases, as often, it is not always clear that a defendant satisfies all three elements. Seemingly the most obvious to claim absence of given its difficulty to prove is the requisite levels of knowledge required of the article alleged to be under possession. Establishing knowledge of possession requires an assessment of the offender's cognitive process, involving the identification of facts, which were readily available to the offender at the time of the alleged offence[416]. For possession to be established, a person must not just demonstrate knowledge of and custody and control over a piece of property, but also demonstrate it to a higher degree than anyone else[417].

So far discussion has remained with the identification of possession of tangible objects, capable of physical interaction, visible to the eye and often easily apparent to those who wish to interact with them. Further difficulties lie when the articles in question are of an intangible nature, specifically in reference to digital data stored within a form of digital storage media, which is considered in the following sections.

4.3 Possession in the context of electronic data/files

Establishing possession of electronic data is key in the context of digital offences and crucial when establishing liability for the offence of possession of IDCSA under the CJA88 s160. To be guilty of an offence of possession, a jury must be satisfied that a defendant is in actual possession of IDCSA. Yet, the element of possession is not defined in any of the statutes relating to IDCSA offences in England and Wales and, as noted above, establishing possession is not a straightforward task. This has given rise to complex issues in this area of law[418] exacerbated by the intricate functionality of computer systems. Given that offenders now use computing technology regularly and IDCSA now predominantly takes the form of digital imagery, establishing possession of this form of data is crucial.

4.3.1 Is data on a digital device intangible or tangible?

In the context of possession of electronic data there are both intangible and tangible elements for consideration of possession[419], as highlighted by Green and Saidov, in reference

[416] R. Fortson, 'R. v Williams (Orette): burden of proof - firearms offence' (2013) Crim. L.R. 983, 985
[417] S. Green, 'The subject matter of conversion' (2010) J.B.L. 218, 221
[418] C. McGlynn & E. Rackley, 'Criminalising Extreme Pornography: A Lost Opportunity' (2009) 4 Criminal Law Review 245
[419] M. Losavio, 'The law of possession of digital objects: dominion and control issues for digital forensics investigations and prosecutions' (2005) Systematic Approaches to Digital Forensic Engineering 177, 177

to computer software and issues of possession surrounding this content[420]. The first question to ask is therefore whether electronic data stored within a hardware device is actually intangible. Intangible can be defined as "unable to be touched; not having physical presence"[421]. Intangible property is frequently described as a 'chose in action' denoting items which are incapable of being possessed[422]. Conversely, tangible can be defined as "a thing that is perceptible by touch"[423]. Although there is limited case law directly discussing the intangibility of digital data specific to IDCSA, in *Your Response Ltd v Datateam Business Media Ltd*[424], generic digital database files were considered intangible, along with computer programmes, considered in *St Albans City and District Council v ICL*[425]. Although Moon[426] indicates a lack of case law discussing tangible digital content, he states that "while a record medium such as a punched card, a magnetic tape, a magnetic disk (hard drive) or a semiconductor chip memory (whether non-volatile ROM or volatile random access memory (RAM)) is necessarily tangible, the information itself is not". This is because although the container (device) can be controlled and touched, the internal digital content cannot be without specialist equipment or software.

The first element for attention is the physical hard disk drive or digital storage media itself. This hardware device stores the information, is physically apparent to the user and it can be touched and removed at any point. However in the realms of investigating IDCSA, it merely constitutes a shell, encapsulating digital data inside. The second element is the actual electronic data residing inside the digital storage media, not viewable to a human eye without specialist software to interpret this content. The question then remains whether just because a person who is in physical possession of a digital storage device, are they also in possession of the data it contains. In terms of tangibility, Green and Saidov [427] attempt to address this issue, but in regards to 'software' (a collection of computer code designed to carry out specific operations) with reference to comments by Justice Hall in *South Central*

---

[420] S. Green & D. Saidov, 'Software as goods' (2007) J.B.L. 161, 163

[421] Oxford Dictionaries, 'intangible' (Oxford Dictionaries, 2014) <http://www.oxforddictionaries.com/definition/english/intangible?q=intangible> accessed 16 February 2014

[422] S. Green, 'The subject matter of conversion' (2010) J.B.L. 218, 221

[423] Oxford Dictionaries, 'tangible' (Oxford Dictionaries, 2014) <http://www.oxforddictionaries.com/definition/english/tangible?q=tangible> accessed 16 February 2014

[424] *Your Response Ltd v Datateam Business Media Ltd* [2014] EWCA Civ 281

[425] *St Albans City and District Council v ICL* [1996] EWCA Civ 1296

[426] K. Moon, 'The nature of computer programs: tangible? goods? personal property? intellectual property?' (2009) 8 European Intellectual Property Review 396, 398

[427] S. Green & D. Saidov, 'Software as goods' (2007) J.B.L. 161, 163

Bell Telephone Co.[428] stating that a distinction between hardware (physical components) and software should not be drawn. Clark states that the software is considered to be 'fixed onto a tangible object'[429]. Further, Green and Saidov [430] highlight a 2 stage possession test for establishing possession of software derived from comments made by Bridge[431] where to be possessed, software must be capable of being exclusively controlled (password protected) and be 'moveable' (can be transferred). Yet, a distinction must be made between software and IDCSA. In reference to IDCSA, such files contain simple binary data and require actual software in order to be viewed.

Where hardware is used as a simple vessel to house software, the act of storing the software on the device in the first instance is likely deliberate (analogous to storing content in a bag) and for the purpose of storing or transferring (for example) the software. However, IDCSA (in reference to computing hardware) may end up residing on a device through multiple intentional and un-intentional acts through general usage, making it difficult to apply similar principles, as the two processes are contextually different.

When a physical hardware storage device is in possession, one could argue that this includes the content inside of the device and the two elements are inseparable (similar to the analogy of a bag holding shopping, noted above, and applicable to cases of software possession). However without the use of computer equipment and the knowledge to use it, the electronic data contained is neither accessible nor viewable, therefore beyond the custody and control of the person, as this information cannot be accessed or manipulated. In addition, without the use of additional specialist hardware and software, the user cannot verify this content. Therefore it is easy to argue that a person at that point in time cannot have knowledge of its content, a key element for establishing possession.

Therefore possession of digital data, specifically IDCSA, maintains two distinct applications of possession. Further, it is not just that an individual needs specialist equipment to access the content stored on a device, but also specialist knowledge to do this. To add to the complexity, accessing all of the data on a device requires varying levels of this specialist knowledge, meaning that depending on how computer-savy a user is will ultimately depend on whether they are capable of controlling all or some of the content on a device. In this

[428] *South Central Bell Telephone Co v Sidney J Barthelemy,* (1994) 643 So. 2d 1240 at 1246.
[429] R. Clark, 'Software agreements, sales law and commercial agents' (2017) C.T.L.R. 23(1) 16
[430] S. Green & D. Saidov, 'Software as goods' (2007) J.B.L. 161, 163
[431] M. G. Bridge, *The Sale of Goods* (Oxford University Press, Oxford, 1997), p.31.

sense the application of the possession requirement of 'control' is not straightforward with further analysis provided throughout the remainder of this chapter.

To provide a high-level overview, to have possession of the intangible data, Clough indicates that a person must display the ability to display, access or interact with this content in some way[432]. This can only be done through computer hardware and software (mobile devices are included). All digital data takes the form of binary or 0's and 1's, which requires a specialist process of interpretation before its content is understandable to the user. As Clough suggests, the difficulty remains that a defendant is in possession of a tangible device, where it must be proved that they are aware that it contains intangible pictures[433]. Of course, in some cases, determining possession of IDCSA on a computing device may be simple (for example, where IDCSA are stored on a user's computer desktop with clear evidence of how it has been used), yet in some instances where deleted IDCSA or IDCSA stored in computer system files may be present, complexity arises. The concept of possession in relation to IDCSA has been debated in a series of cases, culminating in the current precedent for possession of digital IDCSA set out in *Porter*[434].

4.4 The current legal position on possession of digitally stored IDCSA - *R v Porter*

In *Porter*[435], a search warrant and subsequent search of the defendant Ross Warwick Porter's home resulted in the seizure of two personal computers. Forensic analysis of both exhibits revealed 3575 picture files and 40 videos, all categorised as IDCSA. 875 of the pictures were deleted along with a number of pictures found to be embedded in system thumbnail files. The defendant was found to be unable to recover the deleted files due to an absence of specialist file recovery software, likewise with the thumbnail images. Although software to carry out such tasks could have been acquired from the Internet, there was no evidence to suggest this had occurred. The case centred on the contentious area of deleted files and possession and provides precedent for the current application of possession of digital files maintaining IDCSA on a computer systems digital storage media.

In directly addressing the concept of possession the following ruling was issued providing the current application of possession in IDCSA cases.

[432] J. Clough, 'Now you see it, now you don't: digital images and the meaning of 'possession'' (2008) 19 Criminal Law Forum 205
[433] J. Clough, 'Now you see it, now you don't: digital images and the meaning of 'possession'' (2008) 19 Criminal Law Forum 205
[434] *Porter* [2006] 2 Cr. App. R. 25
[435] *Porter* [2006] 2 Cr. App. R. 25

> "… possession, as a matter of law… means having something under your custody or control with the knowledge that you have such a thing in your custody and control" [436]

Porter[437] maintains the current elements found in previous tests of possession for cases of possession of digital files stored on a computer, namely 'custody', 'control' and 'knowledge'. Despite *Porter*[438] providing a number of contentious areas for debate due mainly to the intricacies of digital data (discussed in Chapter 5), it continues to offer a precedent for cases of possession of IDCSA[439], and as a leading case in this area, merits further discussion.

4.4.1 The Elements of the *Porter* Possession Test

Porter[440] suggests that when establishing possession of IDCSA, consideration must be given to the extent to which a defendant has '*custody and control*' over the illegal material. Further, to have custody and control, the defendant also must have knowledge of the fact they have the material under their custody and control[441]. In short, the defendant must know they are in possession of the material and that material must be accessible at the time (so that control over it could be implemented)[442], as previously stated in the case of *Atkins*[443]. In order to appreciate the intricacies involved in the application of the *Porter*[444] possession test, each of its elements are now discussed in turn.

4.4.2 Custody, Control and Accessibility

In considering the need for the element of custody and control, the court made reference to both Lord Diplock[445] and Lord Scarman's[446] interpretations of possession, albeit in the context of drug offences. In both cases, emphasis was place on a need for physical control or custody for possession. As already discussed, digital data is considered intangible, therefore establishing custody and control is not straightforward. Instead, custody and control must be considered in terms of accessibility; which if a file is accessible an individual therefore has

[436] *Porter* [2006] 2 Cr. App. R. 25 at 8.
[437] *Porter* [2006] 2 Cr. App. R. 25 at 8.
[438] *Porter* [2006] 2 Cr. App. R. 25 at 8.
[439] *MacLennan (Hector Colin) v HM Advocate* [2012] HCJAC 94
[440] *Porter* [2006] 2 Cr. App. R. 25 at 8.
[441] *Porter* [2006] 2 Cr. App. R. 25 at 8.
[442] *Porter* [2006] 2 Cr. App. R. 25 at 14.
[443] *Atkins v Director of Public Prosecutions* [2002] 2 Cr App R 248 , 261–262
[444] *Porter* [2006] 2 Cr. App. R. 25 at 8.
[445] *DPP v Brooks* [1974] AC 862 , 866H
[446] *R v Boyesen* [1982] AC 768 , 773H

custody and control over (with the ability to execute, view, move, distribute etc.) the files using their digital device.

The court of appeal in *Porter*[447] stated that a key aspect of possession is that for a file to be possessed it must be accessible using the current capabilities of the computer and any specialist software installed. Further, the file must be accessible at the time of the alleged possession[448]. Therefore, despite 'custody and control' appearing to be the key terms, the test seems in reality to hinge on the accessibility of files as to assert control digital data, it must be susceptible to manipulation or be available for the user to view or access[449].

To add to the complexity of establishing possession, when attempting to identify whether a person has custody and control over IDCSA, an offender's knowledge of the articles also plays a role.

4.4.3 Knowledge

In order to establish custody and control, it is necessary for the defendant to know they have custody and control over the article in question, making knowledge a key aspect in *Porter*[450].

In returning to the aforementioned case of *Cheung*[451] to provide an informative example, it was held, as a starting point, that it must be proven that a defendant knew the article was in existence before possession could be established. Here, the defendant was carrying a bag that they knew contained DVDs. Knowing of their existence in the bag and the ability to access them meant custody and control was established. However, knowledge provides a contentious area for debate surrounding the application of possession when targeted at digital files. Given the intricacies of digital devices and digital data, questions must be raised regarding the application of the knowledge element in the test of possession and the difficulties in applying this subjective test consistently to offenders. The element of knowledge must therefore be examined further.

[447] *Porter* [2006] EWCA Crim 560; [2006] 2 Cr. App. R. 25
[448] Y. Akdeniz, 'Possession and dispossession: a critical assessment of defences in possession of indecent photographs of children cases' [2007] Crim. L.R. 274, 280
[449] J. Clough, 'Now you see it, now you don't: digital images and the meaning of 'possession'' (2008) 19 Criminal Law Forum 205
[450] *Porter* [2006] 2 Cr. App. R. 25 at 8.
[451] *R. v Ping Chen Cheung* [2009] EWCA Crim 2965

4.4.4 What Level of Knowledge is Necessary?

As discussed previously, some offences of possession do not require knowledge of the type or content of the article in question (illicit substance or firearm possession). Regarding IDCSA possession offences, Clough states that different jurisdictions require varying degrees of knowledge, some requiring knowledge of custody and control and of the nature of the image (Canada, US) and others simply knowledge of custody and control of the image (England and Wales)[452]. Clough[453] indicates that English law implements the most limited mens rea requirement surrounding possession of IDCSA offences.

Knowledge denotes the culpability element of the offence of possession and focusing on the position in English law, it has previously been argued that IDCSA offences are one of strict liability (where liability is entailed even in absence of mens rea), in absence of a mens rea element to the offence being defined in statute. In *Atkins v DPP; Goodland v DPP*[454] the position was originally taken that possession was an offence of strict liability and that any possession of IDCSA files would constitute an offence. However, on appeal, this position was overturned[455] and it was held that possession required actual knowledge of the photograph that existed[456].

> … Knowledge is an essential element in the offence of possession under section 160 so that an accused cannot be convicted where, … he cannot be shown to be aware of the existence of a cache of photographs in the first place … Returning to section 160(2)(b), it seems to me indeed that the very fact that Parliament created a defence for those possessing photographs reasonably not known to be indecent, strongly suggests that there was no intention to criminalise unknowing possession of photographs in the first place.[457]

Gillespie[458] confirms that the offence of possession of IDCSA is not one of strict liability, despite the relevant statutes making no reference to mens rea, where the case of *Collier*

[452] J. Clough, 'Now you see it, now you don't: digital images and the meaning of 'possession'' (2008) 19 Criminal Law Forum 205
[453] J. Clough, 'Now you see it, now you don't: digital images and the meaning of 'possession'' (2008) 19 Criminal Law Forum 205
[454] *Atkins v DPP; Goodland v DPP* [2000] ALL ER 425
[455] *Atkins v DPP; Goodland v DPP* [2000] 2 Cr. App. R. 248 at 262
[456] L. Edwards & Waelde, C., *Law and the Internet* (Hart Publishing, 2009)
[457] *Atkins v DPP; Goodland v DPP* [2000] 2 Cr. App. R. 248 at 262
[458] A. A. Gillespie, 'Child pornography: balancing substantive and evidential law to safeguard children effectively from abuse' (2005) 9.1 E. & P. 29,38

supports the notion that an individual must have knowledge of the IDCSA in order to be in possession of them[459]. Selfe[460] indicates that the prosecution must show the "defendant knew of the image's existence, but not necessarily that the defendant knew of the nature of the image". It is then for the defendant to show, on the balance of probabilities that they had not seen, know or had cause to suspect that the picture in question was indecent before being acquitted of the offence of possession under CJA88 section 160[461]. At which point, the defendant must rely upon the statutory defences with the standard of proof being that of the balance of probabilities. Although it is clear that identifying knowledge is a key part of establishing the offence, determining whether a suspect has it, is not a straightforward task and may differ depending on an individuals computer literacy.

4.4.5 Determining a Defendant's Computing Knowledge

The process of establishing knowledge is not without its difficulties and has led to inconsistent judgements as to whether a defendant is actually deemed to be in possession[462]. As knowledge is key to determining possession, establishing whether a defendant has it is a question of fact, left to the jury to determine. Only then "if the jury are sure that the defendant was knowingly in possession of an illegal image in the above sense then the burden shifts to the defendant to establish on the balance of probabilities that the matters making up the statutory defence"[463]. Essentially to establish whether a defendant has the requisite knowledge requires the jury must perform a subjective assessment of the defendant's computing skillset in an attempt to evaluate how computer literate the defendant is. Michaels[464] notes that the difficulty posed by establishing knowledge requires the performance of 'questionable legal gymnastics in order to prosecute'.

It was noted in *Porter*[465] that the need to establish knowledge is crucial to ensure a fair assessment of the defendant's culpability is given. Applying a definition of possession to the offences of possession of IDCSA without establishing knowledge (essentially almost a strict liability application of the law), in the context of computer systems would provide complex

[459] *R* v *Collier* [2005] 1 WLR 843
[460] D. Selfe, 'Extreme pornographic images - mens rea and defences' (2011) Crim. Law. 4
[461] Y. Akdeniz, 'Possession and dispossession: a critical assessment of defences in possession of indecent photographs of children cases' (2007) Crim. L.R. 274, 280
[462] F. S. Monterosso, 'Protecting the Children: Challenges that Result in, and Consequences Resulting from, Inconsistent Prosecution of Child Pornography Cases in a Technical World.' (2009) 16 Rich. JL & Tech. 1
[463] *R. v Ping Chen Cheung* [2009] EWCA Crim 2965 at 15
[464] R. Michaels, 'Criminal Law-The Insufficiency of Possession in Prohibition of Child Pornography Statutes: Why Viewing a Crime Scene Should Be Criminal.' (2008) 30 W. New Eng. L. Rev. 817, 818
[465] *Porter* [2006] 2 Cr. App. R. 25 at 16.

issues and could lead to an influx of prosecutions, which may not in all circumstances be warranted. There is no doubt that the usage of computing technology has increased, yet it can be argued that many users lack an in depth understanding of the underlying functionality of the system itself. Given that many simple user interactions on a computer can trigger thousands of core system events, which are often unknown to the user; such an event may be capable of creating IDCSA unbeknown to the user. Therefore, it is arguably unjust to prosecute for an act which the user may not have knowingly done or understood. Such tasks include that of browsing the Internet where pop-up or redirect websites (where a user is shown or automatically directed to a website they did not intend to access) may occur from which multiple pictures may be downloaded to the users system cache (discussed in Chapter 5). It is feasible for many users to have minimal knowledge of these files therefore indicating a need for knowledge.

Computer systems are complex and multifaceted, where files can be created and stored in many locations due to a number of events. What must be appreciated is that these events could be triggered by both the user through an intentional act on the computer, or, automatically, without user's interaction, awareness or even understanding (an underlying system event). These actions are best summed up by the following comments of Lord Justice Dyson in *Porter*[466].

> "What is in the box is a hard drive. Within the hard drive there are files. Files in the hard drive may or may not include an index. Files are of three categories, operating files, application files and data files. For the purposes of this submission the photographs are, of course, data files and not application or operating system files.
>
> If a file is an active file then, in my judgment, the evidence has established that the user of the computer can without any real difficulty activate and engage the contents of the file on the hard drive; but, in my judgment, a file remains on the hard drive even if it has been deleted or lost because the evidence of Mr Douglas before the jury has been to that effect. A file does not cease to be a file on a hard drive if it has been deleted. It remains a file, albeit a deleted file.
>
> Therefore, the court interprets the word 'possession' in this sense; that the defendant possessed the files within his computer whether they were in an active category or a deleted category."[467]

[466] *Porter* [2006] 2 Cr. App. R. 25
[467] *Porter* [2006] 2 Cr. App. R. 25

Porter[468] requires the defendant to know of the existence of the illegal files before they can be classed as in possession. Yet, there still appears to be ambiguity surrounding the significant issue concerning the defendant's level of knowledge, in particular, the level of knowledge needed to constitute possession. Ormerod [469] suggests that possession is dependant upon knowledge, the effect of which is that depending on where images are found on a computer system, possession could be constituted in different cases. This means that illegal material that resides in complex areas of a computer system will most likely require the defendant to have a higher requisite knowledge of computing technology before possession is established. In contrast, IDCSA found on an offender's computer desktop or documents folder (two areas on a Microsoft Windows Operating System easily accessible by a user), require minimal requisite computing knowledge.

The requirement of knowledge also provides an opportunity for two defendants to carry out the same activity, where prosecution may only occur in one instance where the defendant is found to be more knowledgeable. The apparent issue here is that the possession test appears to protect those who use computer systems but remain ignorant of their functionality. This means that establishing the knowledge requirement of the possession test can be challenging and may lead to inconsistent and unfair results. Given that establishing knowledge is difficult, the jury may look to facts such as the defendant's job, which may prejudice juries and impute knowledge. For example, if a defendant is a computing professional with an understanding of computing technology, it is questionable as to whether a jury's preconceptions may effectively make the offence of possession one of strict liability[470]. In such cases, even the available defences under CJA88 s160(2) would offer limited assistance.

Monaghan[471] highlights that "jurors may violate judicial directions, neglect their duties or displaying prejudices harming public confidence and posing a substantial risk to the integrity of jury trial". In certain crime types, Gobert indicates that juries have a tendency to convict despite evidence that suggests innocence[472]. This is thought to be particularly apparent in

[468] *Porter* [2006] 2 Cr. App. R. 25
[469] D. C. Ormerod, 'Indecent Photograph of a Child' [2006] *Crim. L. R*. 748, 750.
[470] L. Edwards & Waelde, C., *Law and the Internet* (Hart Publishing, 2009)
[471] N. Monaghan, 'The problem of jury misbehaviour in an internet age: recent cases and the Law Commission's consultation' (2013) 18.1 Cov. L.J. 73
[472] J. J. Gobert, 'The peremptory challenge - an obituary' [1989] Crim. L.R. 528

cases involving sexual abuse due to the emotive nature and stigmatisation[473], preventing a jury from remaining impartial[474]. It is questionable as to whether juries can be trusted to correctly determine knowledge and possession in offences of IDCSA because of their emotive nature and general heighten perception of protecting a child, as noted in Chapter 1. A particular concern is that juries may impart a greater degree of knowledge on a defendant particularly if they are aware of software such as wiping applications. Non-technically minded jurors may find it substantially difficult to determine knowledge. Older jury members may be particularly vulnerable due to limited exposure to technology whilst in education. Given that the UK Government has acknowledged plans to raise the maximum jury ages to 75[475], it may not be appropriate for older persons to sit on the jury in pornography possession cases. Yet similar concerns with regards to juries have been raised for a range of offences, particularly in cases containing complex evidence and expert testimony[476].

There are no definitive standards set to judge a defendant's knowledge of their computer; a subjective assessment is simply carried out. It is also arguable that the computer user with a greater degree of knowledge may find it easier to claim to be ignorant of the files in question given that they fully understand the consequences of their actions on their system. This problem is one which is likely to persist, and considerations must be given towards identifying factors that can help a jury accurately attribute knowledge. As technology continues to play a greater role in society, a jury must consider its impact upon the element of knowledge.

4.5 Role of Technological Developments and 'Knowledge'

Arguably, the element of knowledge was easier to establish before the popularity of computing increased. As computer systems were sparse amongst society in comparison to what is now witnessed, the distinction between a non-computer literate individual and a computer expert was greater. However, now with such an abundance of systems, this distinction is no longer so clear.

[473] K. Gant, 'Crying over the Cache: Why Technology has Compromised the Uniform Application of Child Pornography Laws' (2012) 81 Fordham L. Rev. 319, 319

[474] N. Vidmar, 'Generic Prejudice and the Presumption of Guilt in Sex Abuse Trials' (1997) 21.1 Law and Human Behaviour 5

[475] C. Coleman, 'Jury age limit to be raised to 75 in England and Wales' *BBC News* (BBC News, 20 August 2013)<http://www.bbc.co.uk/news/uk-23764925?utm_source=dlvr.it&utm_medium=twitter> accessed 20 August 2013

[476] J. D. Griffith, T. M. Libkuman & D. A. Poole, 'Repressed memories: The effects of expert testimony on mock jurors' decision making.' (1998) American Journal of Forensic Psychology

Technology now plays a significantly larger role in many lives and the sales figures of personal computers have experienced a substantial growth over the past twenty years. Knowledge of computing is at an all time high and information technology is now a significant part of school curriculums with plans to introduce it to children as young as five[477]. The average computer user is now arguably comparative to the computer expert of ten or fifteen year's prior. Therefore it is questionable as to whether everyone who has now undertaken compulsory education possesses enough knowledge automatically to infer the requisite degree of knowledge for possession of files on their system. Although doubtful, one thing that is clear, people now have a greater understanding of the way that their digital devices function, with computing now forming part of education curriculums from an early age.

There appears little guidance and literature published on the subject of determining knowledge in this context and a number of issues are apparent. First the comparison between the computer hobbyist or enthusiast and the computing academic student must be made.

The first possesses no formal qualifications; merely a vested interested in technology and devotes time to understanding their system. The other engages in an academic process, graduating with knowledge of their taught curriculum. In this case, the enthusiast may possess significantly more knowledge, but without formal qualifications, it may be difficult to prove. Conversely, does attaining a computing based degree automatically impart the requisite level of knowledge onto the suspect? Given this scenario, it is arguable that a jury may find it easier to determine knowledge based on the factual existence of a degree certificate. However, it could be argued that any difficulties faced by a defendant may be mitigated by the requirement to obtain permission from the Director of Public Prosecutions (DPP) to prosecute, but this is unlikely to offer much assistance in reality [478]. Here, the DPP could intervene in cases where prosecution would not be in the public interest. Yet, reliance on DPP intervention alone is still an unsuitable compromise for dealing with the difficulties

[477] S. McCaskill, 'New National Curriculum To Teach Five Year Olds Computer Programming' (TechWeek, 2013) <http://www.techweekeurope.co.uk/news/national-curriculum-ict-education-computing-121214> accessed 20 August 2013

[478] S. Easton, 'Criminalising the Possession of Extreme Pornography: Sword or Shield?' (2011) 75 JCL 391

caused by establishing possession. In turn, decisions made by the DPP in practice may fail to identify the true facts of a case and therefore prevent unjust prosecution.

Another consideration relies upon the way in which a user interacts with their digital device. Many users can carry out complex computer based tasks, but this does not always impart the requisite understanding of their device to constitute knowledge. Interacting with applications on a computer is only half of the issue; it is the underlying changes on the operating system, triggered by the users actions which require true computing knowledge in order to fully understand. Many complex tasks require knowledge of that particular domain or system area. Possessing this knowledge does not mean that an in-depth knowledge of other system areas is present with the defendant. This means that when considering the defendant's knowledge as part of the possession test, files found in different areas of the computer operating system require varying levels of consideration. There are a number of particularly contentious computing areas; the most prominent are arguably deleted pictures and files stored within the Internet browser cache[479] along with the difficulties caused by online 'pop-ups' as demonstrated in the case of *Harrison*[480]. Each of these areas arguably require varying standards of computing knowledge to understand the function of a computer system and in turn be in possession of images.

Clough also states that what is termed, as 'de facto' custody must be considered. Highlighted in the case of Canadian case of *Daniels*[481], de facto custody describes a situation where although not in actual physical possession of an article, the defendant in question is the sole possessor of knowledge needed to gain access to them[482]. A common example would involve the use of encryption to obfuscate data where the defendant only knows the password. The Regulation of Investigatory Powers Act 2000 now governs this scenario. These scenarios raise significant issues when applying a test of possession to IDCSA and all are discussed in detail in Chapter 5.

4.6 Concluding Thoughts - A Focus on Computer Systems

Establishing possession of IDCSA is now a difficult task, due to technological developments and the transition in media from physical to intangible digital files. Although the test of

[479] K. Gant, 'Crying over the Cache: Why Technology has Compromised the Uniform Application of Child Pornography Laws.' (2012) 81 Fordham L. Rev. 321
[480] *R. v Harrison (Neil John)* [2007] EWCA Crim 2976; [2008] 1 Cr. App. R. 29
[481] *Daniels* [2004] NLSCTD at [33]
[482] J. Clough, 'Now you see it, now you don't: digital images and the meaning of 'possession'' (2008) 19 Criminal Law Forum 205

possession has remained in its current form for some time, there are arguably key areas for debate surrounding that of requisite knowledge. Given this underlying system functionality within computers, on face value the inclusion of knowledge, as an element of the test for possession noted in *Porter*[483] seems sensible. However in introducing knowledge, the courts have arguably strayed into a significant grey area or subjectivity where it becomes almost impossible to accurately determine a defendant's skill set. Therefore to establish knowledge of the content, the data itself must be examined to look for evidence that the suspected possessor has accessed or manipulated it in order to impute knowledge of it. To enhance the focus of this thesis further, there are two distinct areas of a computer system posing challenges to legal professionals; deleted content and files in the Internet cache.

File deletion is the main way in which a user can part possession with IDCSA, therefore no longer being in custody and control of the illegal content. However there are a number of issues with this process. All deleted files were once live on a given computer system, yet identifying how long the user had possession of them for prior to deletion in many cases is difficult. It remains possible for offenders to possess IDCSA for periods of time prior to deletion, viewing such articles numerous times before deleting them in an aid to part possession. In addition, files in the Internet cache constitute evidence of what the user has browsed online and the websites that they have visited. In essence the cache is a representation of the user's online actions. Despite the cache being the result of a user's actions online, they can only possess this content if they know of its function.

The concepts of file deletion and Internet cache content are considered in depth in Chapter 5 and the implications it pose when attempting to establish possession. Further, Chapter 5 will demonstrate the intricacies of digital evidence and how forensic analysis of digital devices can support the application of the current possession test for IDCSA.

[483] *Porter* [2006] 2 Cr. App. R. 25

Chapter 5

Possession of IDCSA and the Problem Areas Caused by Digital Technologies

5.1 Introduction

In chapter 4, a discussion of the offence of possession has been presented including a breakdown of the possession test and the necessary elements of custody, control and knowledge. Chapter 5 provides an analysis of the challenges of applying the test of possession of IDCSA, focusing on those who possess digital IDCSA on computer systems (with brief consideration given to mobile technologies as discussions in this area are beyond the confines of the thesis). Key problem areas are highlighted, with focus maintained on establishing possession of IDCSA in the deleted areas of a digital device, the Internet cache and encrypted content. These three areas have given rise to numerous complexities in this area of law in a number of cases in England and Wales and will be examined in this chapter. To commence, a discussion of digital forensics is offered due to the field's involvement in offences of IDCSA and the evidence it provides during investigations to support the application of law.

5.1.1 An Introduction to Digital Forensics

The transition to a society dependant on digital technology has now seen much of the evidence found in cases of IDCSA take a digital form, requiring the expertise of digital forensic practitioner to interpret [484]. Offences surrounding IDCSA often involve large quantities of digital evidence on a diverse range of devices, in need of exploration and interpretation in order to establish a chain of events, which have occurred on a suspect device [485]. The discipline of Digital Foreniscs (DF) involves the acquisition, analysis and interpretation of digital data stored on digital storage media [486]. For example, DF practitioners can recover data in 'cache files, swap files, temporary files, unallocated space, or slack space. Browser histories, address books and date and time stamps which can also be

[484] P. Sommer, 'Evidence in Internet paedophilia cases' (2002) 8.7 C.T.L.R. 176
[485] P. Sommer, 'Evidence in Internet paedophilia cases' (2002) 8.7 C.T.L.R. 176, 176
[486] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd, Academic Press 2011)

useful sources of evidence"[487]. An investigation can establish patterns of suspect behaviour and the ways in which a suspect has interacted with their system[488]. Crucially, digital evidence can often provide evidence that can determine a suspect's intentions when using their system and in turn, whether they have intentionally acquired and accessed particular files and their content. This is decisive when trying to establish how IDCSA material has come to reside on a system. In the context of investigations into the suspected possession of IDCSA, forensic procedures can be used to extract all recoverable IDCSA on a system whilst in some cases offering an explanation as to how these files got to reside there and potentially providing evidence of the users custody, control and knowledge of any IDCSA in question. In order to successfully prosecute those suspected of possessing IDCSA on a digital device, reliance is placed upon digital forensic evidence to indicate whether a user had possession of IDCSA on their device.

To begin, this chapter examines IDCSA found in the deleted area of a digital device and their potential to be possessed.

5.2 Problem Area 1: Deleted Files

Deleted files pose a challenge to the possession test, and conflicting views were expressed between the Crown and Appeal courts in *Porter*[489]. Despite a suspect being in possession of a computer and therefore the hard disk drive containing digital data, more information is needed in the context of IDCSA possession offences. It is not enough to have physical possession of the device; a suspect must also be capable of possession of the data residing on it[490]. Following the Court of Appeal's judgement in *Porter*[491], it is for the jury to determine if deleted IDCSA were accessible by the defendant, considering all the factors in the case, which include the defendant's knowledge and particular circumstances along with available DF evidence[492]. Typically this would involve identifying whether the defendant possessed software capable of deleted file recovery. In order to establish the difficulties that deleted files pose to the user, an understanding of the file deletion process must first be acquired.

[487] R. E. Bell, 'The prosecution of computer crime' (2002) 9.4 J.F.C. 308
[488] P. Sommer, 'Evidence in Internet paedophilia cases' (2002) 8.7 C.T.L.R. 176
[489] *Porter* [2006] EWCA Crim 560; [2006] 2 Cr. App. R. 25
[490] *Porter* [2006] EWCA Crim 560; [2006] 2 Cr. App. R. 25 and A. Antoniou, 'Possession of prohibited images of children: three years on' (2013) 77.4 J. Crim. L. 337, 338
[491] *Porter* [2006] EWCA Crim 560; [2006] 2 Cr. App. R. 25
[492] Y. Akdeniz, 'Possession and dispossession: a critical assessment of defences in possession of indecent photographs of children cases' [2007] Crim. L.R. 274, 280

5.2.1 How File Deletion Works

Digital storage media (DSM) can take many forms, ranging from the hard disk drive in typical home computers to flash storage memory, in the form of USB (Universal Serial Bus) memory sticks. In most cases, the process of file deletion is similar. To store files on DSM, it must be first formatted with a file system. An appropriate analogy would be to compare the file system with that of a library filing system. The file system on DSM allows a computer operating system (OS) to locate and access files, which are stored upon it, similar to a library's book catalogue system. A typical example would involve a defendant storing five picture files on their Microsoft Windows 10 home PC. The OS can access the file system on the DSM and obtain information relating to where the file is stored. In turn the OS can then access the file and make it viewable to the user on command. The file system allows the user to view and access every file stored on their system. When a file is deleted, the details regarding its location on the DSM are removed and are no longer accessible by the user (without the use of specialist software). Simplistically, the file can be thought of as 'lost' and the OS is unable to locate it. The contents of the file now reside in the deleted areas of the DSM, referred to as the unallocated clusters and the file is then referred to as deleted. The unallocated clusters of a device can be thought of as an unregulated collection of data which was once live on the computer system but has since been deleted. There is no defined structure and files of any type (once deleted) could end up here. The interpretation of this information is challenging and recovering a file is not simple.

File deletion also provides problems if significant usage of the computer has taken place after deletion; the pictures may be overwritten and therefore unrecoverable using current forensic methods[493]. Overwriting occurs when original file data is replaced with new file data. When this occurs, the original data cannot be recovered. When a file is live on a system, its content protected until it is deleted. Once deleted, the space the file occupies on the DSM becomes available and vulnerable to being used and therefore overwritten by a new file. The contents of the deleted file are at the mercy of the user, with the greater the amount of user activity (creating new files), the greater the chance of the deleted file becoming overwritten.

When a file is deleted, the amount of information available about it diminishes. Live files contain information known as file system metadata, which can be interpreted by a digital

[493] G. Betts, 'Powers of Criminal Courts (Sentencing) Act 2000: Committal for Sentencing.' (2012) 76 J. Crim. L. 12

forensic expert. The benefit of this is that an expert can tell when a live file is created, last accessed and potentially how long it has resided on the system for. In turn the movements of a file can be tracked, including where it originated from and crucially, whether it has been viewed and acknowledged by the user. When a file is deleted, all this information is often lost meaning that all an expert can tell about a file is that at one stage in time (however this time often cannot be accurately established), the file was once live.

Deleted files also maintain ambiguity regarding their access due to the nature of the way that OSs' work. When a file is modified, accessed or created on a computer system, it is given a time stamp denoting the files activity. For example, a file created on the 1st January 2011 is stamped with this time. When the file is modified, a separate time stamp is generated to reflect the time this occurs. Finally and possibly most crucial in relation of possession offences is the 'last accessed' time stamp, denoting the last time a user has interacted with the file in question. When a file is live, DF specialists can acquire these time stamps. When the user deletes the files, all this information is lost. In addition, information regarding the name of the file and where it resided on the system when it is live is also gone. In essence, it is not possible with 100% certainty to tell when a deleted file was last viewed or where it came from when it was live. This is a key annoyance with deleted file data, as everything that resides in the unallocated area of DSM was at some point in time, live, and could contribute to establishing an offence of possession of IDCSA. This was the issue in *Rowe*[494] and DF experts could not say whether the deleted files had ever been viewed.

When considering deleted files, attention must also be given to the deletion process. Typically when a user deletes a file, it passes into the 'Recycle Bin' or equivalent on non-Microsoft systems (i.e. Trash on Macintosh computers). This feature is a failsafe protecting those who accidentally delete files and preventing their content from becoming lost. A user can then proceed to access the Recycle Bin and restore the files back to their original place on the system (prior to deletion), making them accessible until the Bin is 'emptied' removing all of the content stored in it. Yet knowledge of this function may not always be apparent to a defendant. This causes an issue, as if a defendant tries to delete a file, it is still technically accessible and therefore potentially under their possession and control, subject to them demonstrating that they did not know deleted files were still stored and accessible in the recycle bin.

[494] *R. v Rowe (Christopher)* [2008] EWCA Crim 2712;

Following this overview of the file deletion process, consideration can now be given as to whether deleted files can be possessed.

5.2.2 Can deleted files be possessed?

At this point it must be emphasised that standard OS's (e.g. Microsoft XP, Vista, 7, 8, 10, MAC OSX, Linux) by default, only provide the user with the ability to access 'live' (non-deleted) files. Therefore pictures residing in the deleted areas of digital storage media are not accessible to a user without first acquiring specialist software, a key requirement of the possession test in *Porter*[495], where currently, deleted files are not normally found to be possessed subject to the comments in Section 5.5. DF experts regularly implement file recovery techniques to recover deleted files using specialist equipment and software, some of which is only available to law enforcement agencies. The cost of this equipment is often substantial. However, now the Internet has allowed access to a range of freeware (software which is accessible without charge) tools, claiming to, and often successful in the recovery of deleted file content. These tools can be easily found through online search engines and in turn downloaded and installed on the machine. In addition, due to the abundance of reference material available on the Internet, a user who searches for the right phrases can easily gain access to information informing them of the correct process needed to recover files. Arguably, understanding the process of file recovery can be thought of as requiring a high level of expertise or expert knowledge, which is often presumed to be beyond the standard person. Yet many freeware recovery tools are designed with simple graphical user interfaces, simply requiring the basic execution of commands to commence a file recovery, requiring no knowledge of how it carries the process out. Therefore given the ease of accessibility to recovery software, it is debatable as to whether deleted files are truly inaccessible to the user. Adding to this problem is the users ability to download and install an application for file recovery, then once it has been used, uninstall it to remove all traces of its use. Therefore in some cases, it may be impossible to tell over a period of time whether deleted files were at one time accessible, but may no longer be.

The problem which is posed in *Porter*[496] is that files must be accessible at the time of seizure. This issue was also discussed in the case of *Rowe*[497]. Here, the defendant was found to have a form of DSM at his parent's house, which after expert investigation, was found to contain 124 indecent images. Yet, forensic practitioners confirmed that in absence of specialist

[495] *Porter* [2006] EWCA Crim 560; [2006] 2 Cr. App. R. 25
[496] *Porter* [2006] EWCA Crim 560; [2006] 2 Cr. App. R. 25
[497] *R. v Rowe (Christopher)* [2008] EWCA Crim 2712;

software, the defendant did not possess any method of accessing them. In absence of this ability the conviction was quashed as the file was beyond their current means of possession. Therefore despite the potential for access by acquiring the software it appears that the software must actually be present on the system at the time possession is brought into question. The issue here is that it can be difficult to establish whether the user has had file recovery software on their machine but has since uninstalled it prior to their device being seized. When software is installed it implements a number of log files and changes on the user's system. When the user chooses to remove this software (carries out an uninstall process) often the software removes all remnants of itself from the machine. This leaves an unknown gap in user activity where a defendant may have had access to deleted files by utilising all of the potential resources available to them, then chose to remove their access to the illicit content by uninstalling the software.

In reality, a suspect seeking to 'store' material in the deleted areas of a drive and access them via recovery tools would seem unlikely, but remains feasible. As noted above, the process in which deleted data becomes overwritten makes for a high potential that general computer usage overwrites the IDCSA and therefore they become inaccessibly by any means. However this scenario is viable if the user chooses to fill a form of removable media (USB stick) with IDCSA and deleted them. As there will be no system processes occurring on this form of storage media, no overwriting of data can occur, therefore, technically they are protected. As a result, the suspect is in possession of a USB stick containing IDCSA, but one, which will appear empty until recovery software is used. The user could then use recovery software every time they wish the view the material then uninstall it after every viewing session. Although this scenario appears highly complex and arguably suspicious, given a suspect who wishes to evade detection for possession offences, all of the tools needed to implement this situation are easily and freely available to a user.

An alternative scenario raises questions whether the presence of file recovery software on a system automatically makes a user vulnerable to possession offences. Given the ease of availability of recovery software (previously noted) it is possible that users may implement these tools for legitimate purposes (recovery of accidently deleted family photos for example). However in doing so, following *Porter*[498], the user has now potentially taken possession of all information in the deleted areas of their device as technically it has become accessible and arguably within their custody and control, with questions of knowledge

[498] *Porter* [2006] EWCA Crim 560; [2006] 2 Cr. App. R. 25

having to be raised. When considered with the complexity of computer systems and the vast quantities of data involved, it may be deemed unrealistic to be fully aware of everything in the unallocated space of the drive. This means that should the user unintentionally acquire IDCSA (deleted from their Internet Browser cache from an accidental visit to a site hosting IDCSA for example), they are technically in possession of it unless they can prove they had no knowledge of it, which may be difficult. It also raises the question that if a user has accidentally downloaded or viewed IDCSA and then deleted it, can they ever implement file recovery software on their system for legitimate purposes without the fear of the IDCSA returning to their possession.

The case of *Miller*[499] provides conflicting and arguably correct assessments. Here, DF investigations had found the remnants of 261 IDCSA in the deleted areas of a hard disk drive, which the defendant claimed were placed there prior to acquisition of the device. The defendant was charged with possession of IDCSA on or before November 20th, 2002. In absence of specialist file recovery software, there was no method of access to the files and, following *Rowe*[500], possession could not be established. However the true extent of DF evidence was utilised. The OS (Windows 98) was found to have been installed on the computer in March 2001 and re-installed again on February 2002. One of the novel features of the above OS is the requirement to type in the name of computer owner during the installation process. The name found to have been entered matched that of the defendant suggesting ownership of the device during a critical time period when the IDCSA were allegedly obtained. The defendant was also found to have used an email address on the system, of which the address resembled that of the defendant's actual name. Finally a number of deleted Internet search history records and Internet search terms were recovered showing obvious access to illicit web sites. Utilising this "evidence at the trial was to prove the knowledge necessary for possession and thus to rebut the defendant's explanations raised by him for the presence of these images on his machine"[501].

In summary, the issues surrounding accessibility lie with the current interpretation of *Porter*[502] resulting in files having to be actually accessible, not potentially. It would appear specialist file recovery software and a suspect's knowledge to utilise it would appear key, and in the absence of it, deleted images remain out of possession of the defendant. This

[499] *R. v Miller (David)* [2010] EWCA Crim 2883
[500] *R. v Rowe (Christopher)* [2008] EWCA Crim 2712;
[501] *R. v Miller (David)* [2010] EWCA Crim 2883
[502] *Porter* [2006] EWCA Crim 560; [2006] 2 Cr. App. R. 25

initially seems to be a sensible approach given that it is presumptuous to apply all those who have access to potential file recovery solutions would intend to use them. Similarly placing deleted files in within the possession of the defendant essentially makes the defence under CJA88 section 160(2)(c) redundant as the only option available to the user to part with the IDCSA before an unreasonable amount of time would be to physically destroy the device.

When discussing possession in the context of deleted files it is necessary to consider the statutory defences available to the defendant. Although currently deleted files are not in possession (therefore no offence of possession is committed) the CJA88 section 160(2)(c)[503] provides a defence to those who acquire IDCSA but then delete it within a reasonable time. Therefore file deletion is currently a form of defence. However, the application of this defence is not itself without issues.

5.3 Deleted Files in the Context of Section 160(2)(c) CJA88

In conjunction with deleted IDCSA, the most appropriate defence to consider at this point is that of unknowing receipt of illicit material and not keeping it for an unreasonable amount of time (i.e. deleting it)[504]. Here, providing the defendant does not keep the material for an unreasonable amount of time, no offence will be committed meaning that a defendant must part with possession of the material (i.e. delete it). However the key problem surrounding the application of this defence is the difficulty in establishing an unreasonable time frame, which Crown Prosecution service guidance suggests that there remains ambiguity as to how long constitutes unreasonable[505].

5.3.1 What is an Unreasonable amount of time?

Determining an unreasonable amount of time is problematic. First, no guidance is provided in statute as to what time framework would be unreasonable and, as stated above, the Crown Prosecution Service guidance is minimal. There are two approaches, which could be taken to adjudge this time. First, the time between the IDCSA's creation and subsequent deletion could be assessed. The second approach is to determine the time from when the suspect identified the file (first viewed its contents) to the time it was deleted. The problem with both these approaches (as previously noted) is that when a file is deleted, all of the time and date information used to make the above assessments is lost. As a result,

[503] Criminal Justice Act 1988, s160(2)(c)
[504] Criminal Justice Act 1999, s160(2)(c) and Criminal Justice and Immigration Act *2008* s65(2)(c)
[505] CPS, 'Indecent photographs of children' <http://www.cps.gov.uk/legal/h_to_k/indecent_photographs_of_children/> accessed 14 May 2015

establishing an unreasonable time, in theory provides a useful benchmark, but in the context of deleted content, it is difficult to establish. This means that DF evidence may not be able to distinguish between a defendant who has maintained pictures for years before deleting them days before arrest, from one who deleted images straight away. It is for this reason the defence has a significant potential to be abused and arguably offers protection to those harbour IDCSA but can quickly delete it.

In essences the statute refers to 'an unreasonable time', which in many situations it is impossible to determine such information with regard to files found to have been deleted. Often, a file's history whilst live on a device is lost once it has been deleted. A DF investigation of DSM can only offer limited assistance, mostly in the form of analysis of logs of activity stored within the OS itself. However, there are two main ways a DF practitioner may be able to track the life of a file to determine its life span and ultimately the presence of the illusive 'unreasonable time'.

5.3.2 Log Files

An analysis of log files can provide an insight into the amount of times and at what point a particular file has been accessed, therefore providing an insight into whether a user has had a file 'an unreasonable' amount of time. An example of this is the index.dat file. This file not only contains Internet history records, but also documents accesses to files stored locally on a computer running the Microsoft Windows OS. Analysis of index.dat files can show how the user has interacted with their system over a period of time. However it will not allow a practitioner to directly correlate activity with deleted files. Instead reliance would be placed on the names of the files stored on the computer. The index.dat files will only show details of file names and file paths (location on the system). If a defendant has files with names indicative of illicit content then the index.dat can provide indications that IDCSA may have been accessed. The timestamps associated with these files could show the user repeated accessing files with suspicious names and in turn infer an unreasonable time. This also raises two apparent issues. First, there is no way of telling whether files with inappropriate names, actually contain illegal content. This connection would be solely based on the contents of the unallocated areas of the DSM and the indicative file names that would be insufficient. Second, the defendant can avert this evidence by simply naming the files stored within their computer names that are inconspicuous.

5.3.3 An Example: Volume Shadow Copies

One form of evidential log file is the Volume shadow copy (VSC), which can be thought of as snapshots of a computer system at intervals in time. Using the Microsoft Windows 7 OS as an example, VSCs are taken on a weekly basis (or when new software is installed) by the system. VSCs are a 'file level' back up, meaning that every time a VSC is taken, all files on the system are captured. A typical system may have multiple VSCs taken over a period of months. The advantage of this is that files, which were live at one point, but have since been deleted may have been snapshotted. Analysis of VSCs can provide a snapshot timeline view documenting the state of the computer over a period of time. A DF practitioner interpreting VSC could identify whether a particular IDCSA has been live for a period of time, which is not reasonable. However, this form of evidence is confined to specific circumstances where the suspect has used a specific OS and may not be available in all circumstances.

5.3.4 Can File Deletion Indicate Possession on its own?

Howard[506] has suggested that deletion of IDCSA could also provide strong evidence for knowing possession of images. Howard's[507] views merit brief discussion.

5.3.5 Volume of Images

The first scenario to consider is where a large volume of deleted IDCSA has been recovered from a system. Hessick[508] has also raised such sentiments, albeit in the context of live images for purposes of sentencing. However, it is arguable that the volume of IDCSA on a computer system could also be considered in the context of establishing possession, particularly in relation to deleted images. Similarity the same concepts are applied in the context of illicit substances in the US. Offences surrounding drug related substances in the US penalise the defendant based on the amount of the illicit substance they possess, where a base line weight is set followed by incrementing punishments depending on how much is found[509]. Although the concept is for the purpose of determining the severity of sentence, it may also hold merit when determining culpability in terms of deleted file possession, working off the presumption that those who are actively involved with IDCSA are likely to have possessed and deleted more than just 'a few' images. This is in comparison to those who stumble upon IDCSA for example, through an act such as a mistyped website which is unlikely to cause the

[506] T. E. Howard, 'Don't Cache out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files' (2004) 9 Berkeley Tech. L.J. 1255
[507] T. E. Howard, 'Don't Cache out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files' (2004) 9 Berkeley Tech. L.J. 1255
[508] C. B. Hessick, 'Disentangling child pornography from child sex abuse.' (2010) 88 Wash. UL Rev. 853
[509] J. J. Exum, 'Making the Punishment Fit the (Computer) Crime: Rebooting Notions of Possession for the Federal Sentencing of Child Pornography Offenses.' (2009) 16 Rich. JL & Tech. 1

download of thousands of IDCSA which would then need to be deleted. Although practically, applying such a principle is unrealistic (due to the points noted below, and in turn as it relies on a rather arbitrary distinction between volumes of IDCSA), it is an attempt to combat the limitations surrounding deleted digital data and should be highlighted.

The issue here is that often there is no way of determining why deletion has taken place; it could either be purely intentional on the part of the user or in turn via an automated system process. It is also difficult to tell where a deleted file came from in many scenarios, presenting a challenge in relation to identifying whether first, a person was in possession of a file and second, whether they actually had the file an unreasonable amount of time. Yet, it is arguable that a user who stumbles upon an illicit webpage and ultimately deletes their cache should only have a limited number of IDCSA in the deleted areas of their drive. A typical webpage may cache anywhere from one and over one hundred images on the system (depending on site structure and content). Yet given the recovery of substantially more images, this may suggest the presence of more than one accidental viewing of IDCSA. Therefore one option for possession in the context of deleted IDCSA is to set a threshold volume, where a user who maintains significantly more IDCSA in their unallocated space is deemed to have once been in possession. An example could state that possession will be established if the user has over a thousand recoverable IDCSA images. The acquisition of one thousand IDCSA is unlikely to occur without the deliberate and intention act of seeking out these images. In addition, this approach prohibits those who delete their archive of IDCSA in fear of being prosecuted by preventing reliance on the defence of keeping the IDCSA an unreasonable amount of time, with this point elaborated on in Chapter 6. However, as noted above, the concept of establishing culpability via volume of IDCSA is unreliable as there is no way to ascertain accurately what caused the volume of IDCSA to be deleted in the first instance. Therefore, this principle protects those who deliberately wanted to download IDCSA but only obtained a small amount of images and would wrongly imply guilt to an instance where an individual unintentionally triggered an event resulting in a large batch of IDCSA being stored on their machine.

5.3.6 A final consideration - Wiping Software

When considering parting possession with a digital file, the most effective method of removing content from a computer system (other than physical destruction of the device,) is to employ wiping software. File wiping software ensures that the contents of a file are

overwritten and therefore no longer viewable, essentially permanently deleting it[510] and wiping software is freely available to download from the Internet[511]. Therefore those who may wish to ensure they remove any traces of IDCSA from their system (including preventing it from remaining in unallocated space) if they have been accidentally downloaded is to utilise software of this type.

However using specialist file wiping software could also be a double-edged sword. On one side, the use of this type of software would demonstrate a defendant's intention to fully part with the images for legitimate reasons. Yet, the *Attorney General*[512]stated that "the use of some programmes may well assist a court to draw the inference that the material erased was illegal and that the reason for erasing it was to thwart the criminal investigation". Additionally, due to the provocative nature of IDCSA offences, juries may be more willing to make an inference that wiping software was used to cover illegitimate actions, invoking suspicion. This presence of file wiping software on suspect devices may become more prevalent as society becomes increasingly aware of their privacy and seek to implement to these technologies more frequently.

5.4 Problem Area 2: The Internet Cache

The Internet poses a unique issue for possession offences, unforeseen at the time of creation of applicable legislation. O'Donnell and Miller highlight this issue.

> "Prior to the Internet, a large child pornography collection would have been indicative of an enthusiast of long-standing, somebody who devoted much time, effort and money to amassing his collection. But the Internet allows an individual to download a huge amount of material in a very short space of time. In other words, a collection of 5,000 images possibly reflects the quality of an individual's Internet connection rather than the effort they expended to painstakingly build a collection." [513]

The act of viewing IDCSA online often leaves behind evidential traces depicting the users online movements within their Internet browsers web cache. Howard[514] suggests that

[510] L. E. Daniel, *Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom* (1st, Elsevier 2011) 62

[511] Piriform, 'CCLeaner - PC Optimization and Cleaning' (CCleaner, 2013) <http://www.piriform.com/ccleaner> accessed 20 August 2013

[512] *Attorney General's Reference* (No.89 of 2004)

[513] I. O'Donnell & C. Miller, *Child Pornography; Crime, computers and society* (1st, Willan Publishing 2007) 58

[514] T. E. Howard, 'Don't Cache out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files' (2004) 9 Berkeley Tech. L.J. 1255

pictures stored within the Internet cache symbolise a record of viewed contraband. However conflicting arguments suggest that the cache is similar to 'window shopping' where no possession of material takes place, only passive viewing[515]. To understand the significance of the Internet cache and possession, it is first necessary to understand how the cache functions.

5.4.1 Functionality of the Internet Cache

The Internet cache is designed to enhance a user's experience by speeding up Internet browsing[516]. To achieve this, the Internet browser first allocates storage space on the users computer system, known as the cache and this area will house cached items (sometimes referred to as temporary Internet files[517]). As the user browses a website, files such as pictures which are embedded into the website page are downloaded (cached) and stored locally on the users machine[518]. The effect of this is that the next time a user views the same webpage, it will load quicker as it takes less time to rebuild the webpage from files stored locally than re-download them from the Internet. The key thing to note is that the cache functions automatically, without user interaction[519]. It is a function of the browser application and designed to occur autonomously, often within seconds of viewing the webpage[520]. The effect of this is that anyone who accidently visits a website will often have its content cached on their machine. In turn, the entire website page is cached, regardless of whether the user has actually viewed its content. This means that despite when the webpage is loaded the user is presented with the top part of the webpage, which is initially viewable, parts of the webpage which require the user to 'scroll' down to view are still cached. This provides a difficult situation where a user may have files cached that they have never actually seen.

If the contents of the cache were viewed, it would commonly be found to contain thumbnail sized (small) pictures and fragments of webpages[521]. Using specialist DF processes, the content of the cache directory can be re-built to recreate the how the original webpage

[515] G. Marin, 'Possession of Child Pornography: Should you be Convicted When the Computer Cache Does the Saving for You' (2008) 60 Fla. L. Rev. 1206, 1207
[516] D. Wessels, *Web Caching* (1st, O'Reilly Media 2001)
[517] J. Sammons, *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics* (1st, Elsevier 2012)
[518] E. Casey, *Handbook of Digital Forensics and Investigation* (1st, Academic Press 2009)
[519] K. Gant, 'Crying over the Cache: Why Technology has Compromised the Uniform Application of Child Pornography Laws' (2012) 81 Fordham L. Rev. 319, 319
[520] A. Juels, M. Jakobsson & T. N. Jagatic 'Cache cookies for browser authentication.' In *Security and Privacy, 2006 IEEE Symposium* on 2006 May 21, 5
[521] J. Sammons, *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics* (1st, Elsevier 2012)

would look like that a user has visited and the time and dates that these visits were initiated. It should be noted that unless the system user has intentionally accessed the cache directory, all cached file contents is as a result of the users Internet browsing activity and all files have been downloaded from the Internet sites visited.

Files which are cached remain within the cache directory until they are deleted in one of three ways[522]. First, web browsers when setting up the cache define a specific cache size in terms of disk size[523]. When the cache is full, cached files get deleted to free up space for new cached contents from more recent visits to websites. This process is automatic and occurs without user interaction therefore the amount of Internet browsing a suspect can affect the amount of cache that is deleted. The second deletion method is to clear the cache using the browser's facility to remove Internet history[524]. If the user chooses to purge their browser history in an attempt to remove traces of their activity, cached content is then deleted and resides in the unallocated clusters (discussed above). The third method involves manual deletion where a user can access the cache area and select which files to delete. In addition, a fourth method increasing in popularity due to privacy concerns is the use of specialist deletion software, which targets Internet caches and removes files. Usually this type of software places cached files beyond the powers of recovery of DF specialists.

5.4.2 Possession of the Cache

The current position of the cache is noted by Ormerod[525] who states, "it is important to spell out immediately that any images that remain in the Internet cache on a computer are in D's possession and he will be convicted under s.160 subject to proof of knowledge" of the cache. Therefore a defendant found to possess knowledge of the cache is in possession of the files residing there. Gant[526] expands upon cache discussions and poses the following questions in relation to the current position in English law when trying to establish possession of the cache:

> Can a user knowingly possess an illegal image if he does not know that the image is saved to his computer or the cache exists? - This is required for establishing possession of the cache.

[522] K. Gant, 'Crying over the Cache: Why Technology has Compromised the Uniform Application of Child Pornography Laws' (2012) 81 Fordham L. Rev. 319, 319
[523] M. Miller, *Special Edition Using the Internet and Web* (1st, Que Publishing 2001)
[524] M. Miller, *Speed It Up! A Non-Technical Guide for Speeding Up Slow Computers* (1st, Que Publishing 2009)
[525] D. C. Ormerod 'Indecent Photograph of a Child.' [2006] *Crim. L. R.* 748, 750.
[526] K. Gant, 'Crying over the Cache: Why Technology has Compromised the Uniform Application of Child Pornography Laws' (2012) 81 Fordham L. Rev. 319, 319

The answer to the above question is no, given the current test of possession, which requires knowledge of the file. No knowledge of the cache means that a user would not be aware that the picture is being saved to their computer. Yet, this appears to leave a significant gap in prosecution, distinguishing between actual possession of the file and possession of the image by sight, once it was viewed in the Internet browser. Those who view illegal content on the Internet but claim no knowledge of the cache cannot possess the cached files. The apparent issue here is that the cache essentially retains evidence depicting the suspects Internet activity and viewing habits[527]. Hence, if the cached images do not exist in any other areas of their system (i.e. a user has deliberately saved and organised the pictures), which would constitute possession, an offence may not be constituted allowing the user the option of viewing IDCSA without being in possession. The need for knowledge of the cache provides an opportunity for defendants to find relief under the current possession test and arguably provides a hindrance when attempting to charge on possession. It leaves the user free to intentionally seek out IDCSA online, where in ignorance of the Internet browsers' function, files in this area are not possessed, despite the potential for evidence of intentional searching being present.

As the cache is only generated from where a user has visited online; evidence showing intentional visits to websites hosting IDCSA would infer an intention to view the material. This leads to the key question, "should a suspect possess the cache regardless of knowledge if intent to access illegal sites is proven?". Common past argument which may have prompted cautious approaches to possession of cached contents is the frequent plea of 'pop-ups'. A pop-up is a webpage that is displayed without the request of a user, either through a malicious script or web link[528]. Therefore prosecution for possession of IDCSA in the cache stemming from a series of pop-ups would be unjust. However, DF analysis of web browsing Internet history is able to distinguish between visits to pages, which are created intentionally, and those that are generated through an autonomous pop-up. DF analysts now possess significant understanding of the functionality of web browsers (for example, Chrome, IE, Firefox) and the artefacts left behind from specific user activities. Yet it appears that the current test for possession disregards this potential beneficial evidence suggesting a user's true intentions when online in preference of a subjective test of knowledge, which is difficult to prove. In turn, CPS guidance suggests a prosecution for making is more

[527] J. Sammons, *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics* (1st, Elsevier 2012)
[528] A. Jones & C. Valli, *Building a Digital Forensic Laboratory* (1st, Butterworth-Heinemann 2011) 108

favourable as it negates the difficulties of establishing knowledge of the cache in favour of clear evidence of intentional searching[529].

5.4.3 The Internet Cache, Deleted Files *Jayson* and the offence of Making

Porter[530] provides that a defendant must have knowledge of the cache in order to establish possession. However this position should be considered in conjunction with the decisions in *Bowden*[531] and *Jayson*[532], cases which address images in the Internet cache.

Bowden[533] stipulates that a defendant who intentionally downloads IDCSA from the Internet to their computer is making IDCSA rather than possessing them as an electronic duplicate of the original picture is created.

> A person who either downloads images on to disc or who prints them off is making them. The Act is not only concerned with the original creation of images, but also their proliferation. Photographs or pseudo-photographs found on the Internet may have originated from outside the United Kingdom; to download or print within the jurisdiction is to create new material which hitherto may not have existed therein. [534]

This point was echoed in the case of *Jayson*[535]. Here, a number of deleted images were found in the defendant's computer cache, recovered by specialist techniques under expert investigation. Given the absence of software for recovering the files, they were not technically in possession. However, the trial judge ruled that the act of viewing images online through the Internet browser, ultimately ending up cached through the browsers automated process was equivalent to the offence of making, provided the necessary mens rea (intent to access the image, proven for example through evidence of online searches) is established[536]. The prosecution in *Jayson*[537] argued that cached images could be re-accessed

---

[529] CPS, 'Indecent Images of Children' <http://www.cps.gov.uk/legal/h_to_k/indecent_photographs_of_children/> accessed 15 January 2016

[530] *Porter* [2006] EWCA Crim 560; [2006] 2 Cr. App. R. 25

[531] *R v Bowden* [2000] 1 Cr.App.R.(S.) 26

[532] *R v Graham Westgarth Smith, Mike Jayson* [2002] EWCA Crim 683

[533] *R v Bowden* [2000] 1 Cr.App.R.(S.) 26

[534] *R v Bowden* [2000] 1 Cr.App.R.(S.) 26

[535] *R v Graham Westgarth Smith, Mike Jayson* [2002] EWCA Crim 683

[536] Y. Akdeniz, 'Case report: Court of Appeal clarifies the law on downloading pornography from the Web.' (2002) 18.6 Computer Law & Security Review 433

[537] *R v Graham Westgarth Smith, Mike Jayson* [2002] EWCA Crim 683

if the defendant wished to do so (although in *Jayson*[538], the defendant stated he had no intention to do so) and in turn, stored in the cache as an attempt to avoid liability[539].

> We reach that conclusion as a matter of the ordinary use of language, and giving to the word "make" its ordinary and natural meaning, as did this court in Bowden. By downloading the image, the operator is creating or causing the image to exist on the computer screen. The image may remain on the screen for a second or for a much longer period. Whether its creation amounts to an act of making cannot be determined by the length of time that the image remains on the screen.[540]

Although the ruling in *Jayson*[541] surrounded deleted images in the cache, which had been acquired from the Internet, the distinguishing feature is the inclusion of the requirement for intention. Akdeniz[542] suggests that the case of *Porter*[543] failed to clarify the law surrounding deleted files and possession where emphasis is placed upon knowledge and the availability of files. It is suggested that this has left an unsatisfactory gap in the offence of possession which Ormerod[544] states needs to be addressed. Akdeniz provides an example of the issues with the possession offence.

> In the scenario of A knowingly downloading indecent images but deciding to delete them with no intention to undelete or recover them, A would expect to avoid possession and could also have a defence, if the images were in a deleted state and unrecoverable by A at the alleged time of possession and A does not have such software or there is no evidence to suggest that A tried to recover the deleted images by such software.[545]

This may leave a charge under the offence of making as opposed to possession where images are found in the cache but are deleted[546]. For example, deleted cached files are not in possession but given evidence of intent, the making offence is established, as it does not matter whether the files are accessible. This also means that where images are in the cache and accessible and with evidence of intent, preference may be to prosecute under a charge

---

[538] *R v Graham Westgarth Smith, Mike Jayson* [2002] EWCA Crim 683
[539] Y. Akdeniz, 'Case report: Court of Appeal clarifies the law on downloading pornography from the Web.' (2002) 18.6 Computer Law & Security Review 433
[540] *R. v Smith (Graham Westgarth)* [2003] 1 Cr. App. R. 13 at 33
[541] *R v Graham Westgarth Smith, Mike Jayson* [2002] EWCA Crim 683
[542] Y. Akdeniz, 'Possession and dispossession: a critical assessment of defences in possession of indecent photographs of children cases' [2007] Crim. L.R. 274, 284
[543] *Porter* [2006] EWCA Crim 560; [2006] 2 Cr. App. R. 25
[544] D. C. Ormerod, 'Commentary on *R. v Porter*' [2006] Crim. L.R. 748.
[545] Y. Akdeniz, 'Possession and dispossession: a critical assessment of defences in possession of indecent photographs of children cases' [2007] Crim. L.R. 274, 284
[546] Y. Akdeniz, 'Case report: Court of Appeal clarifies the law on downloading pornography from the Web.' (2002) 18.6 Computer Law & Security Review 433

of making as it evades the complexity of establishing a defendants knowledge but also prevents the defendant from having access to any of the statutory defences.

The key issue for discussion here is that arguably making is a more serious offence than possession given that possession carries a maximum penalty of five years in comparison to ten for making as amended by the Criminal Justice and Court Services Act 2000. The courts generally recognise possession as the lowest form of culpability in the range of IDCSA offences[547] yet the line between possession and making is now blurred. Akdeniz[548] suggests that the decision in *Bowden*[549] surrounding making and the Internet cache should be revisited. Gillespie[550] suggests that although on literal interpretation, the act of an Internet browser caching files is 'making', the act itself is more analogous to the possession offence. Further, it is suggested that at the time, the decision in *Bowden*[551] was born of necessity in order to evade the defendant being subject to a maximum penalty of six months (at that point in time), which was considered paltry in comparison to the amount, and nature of the IDCSA, which was downloaded[552]. However, given now that penalties are more severe for possession of IDCSA, the author argues that the case of *Bowden*[553] should be reviewed and this will be addressed in Chapter 6.

The definition of making suggests some form of deliberate and intentional act. However the creation of pictures in the cache is not intentional, it is autonomous. In addition, when the making offence was created, it was arguably done so to prosecute those who are present or involved during the original physical abuse as part of the image creation, due to limited technology and the use of the physical as opposed to digital photography as the main means of creating the IDCSA. However, now that digital data makes 'creating/making' new IDCSA easier, where often there is no personal involvement in the original abuse often where the defendant is a substantial distance away from these events, it appears incorrect to apply the same penalty. Making the original IDCSA and making a copy are significantly different and

[547] J. J. Exum, 'Making the Punishment Fit the (Computer) Crime: Rebooting Notions of Possession for the Federal Sentencing of Child Pornography Offenses.' (2009) 16 Rich. JL & Tech. 1, 32
[548] Y. Akdeniz, 'Case report: Court of Appeal clarifies the law on downloading pornography from the Web.' (2002) 18.6 Computer Law & Security Review 433
[549] *R v Bowden* [2000] 1 Cr.App.R.(S.) 26
[550] A. A. Gillespie, 'Indecent images of children: the ever-changing law.' (2005) 14.6 Child Abuse Review 430
[551] *R v Bowden* [2000] 1 Cr.App.R.(S.) 26
[552] A. A. Gillespie, 'Indecent images of children: the ever-changing law.' (2005) 14.6 Child Abuse Review 430
[553] *R v Bowden* [2000] 1 Cr.App.R.(S.) 26

perhaps a better approach is to implement the need for intention into the current definition of possession and a further discussion of this is seen in Chapter 6.

5.5 Problem Area 3: Encryption and the Regulation of Investigatory Powers Act 2000 (RIPA)

The final problem area for consideration is that of encryption, and its ability to obfuscate digital data providing for significant difficulties when attempting to establish possession of digital IDCSA.

The UK Government introduced RIPA in order to regulate surveillance techniques and the interception of communications [554]. However this legislation provides a key tool for preventing offenders from escaping conviction through the use of encryption techniques[555]. Encryption involves the obfuscation of information via a computational algorithm, often implemented for purposes of security and protection of information[556]. Encryption can also be implemented for malevolent purposes, particularly to hide the remnants of a digital crime. Digital storage media holds data in a binary format, which is interpreted by computing software and transformed into a format, which is visually understandable. Encryption software can take this data and scramble the contents using mathematical algorithms rendering it unreadable[557]. Without an encryption key, essentially a password used to reverse the algorithm returning the data back to its original state, the file remains in an unreadable state[558]. Encryption provides the user with privacy and protection for their data, ensuring that should it get lost or stolen, it cannot be easily acquired or abused. There are strong arguments for the legitimate use of encryption and Microsoft; a leading organisation in computer software manufacturing now provides users with full disk encryption (encrypt the entire system hard drive) facilities since the production of their Windows Vista, 7 and 8 operating systems (OS). However, conversely encryption provides a defendant with the ability to obfuscate illicit material and place it beyond the reach of authorities.

---

[554] Y. Akdeniz, N. Taylor & C. Walker, 'Regulation of Investigatory Powers Act 2000 (1): Bigbrother.gov.uk: State surveillance in the age of information and rights.' [2001] Criminal Law Review 73

[555] B. B. Chatterjee, 'New but not improved: a critical examination of revisions to the Regulation of Investigatory Powers Act 2000 encryption provisions' (2011) 19.3 Int J Law Info Tech 264

[556] Microsoft, 'What is Encryption?' (Windows, 2014) <http://windows.microsoft.com/en-gb/windows/what-is-encryption#1TC=windows-7> accessed 20 January 2014

[557] B. B. Chatterjee, 'Fighting Child Pornography through UK Encryption Law: A Powerful Weapon in the Law's Armoury.' (2012) 24 Child & Fam. L. Q. 410

[558] D. J. Sherwinter, 'Surveillance's Slippery Slope: Using Encryption to Recapture Privacy Rights.' (2006) 5 J. on Telecomm. & High Tech. L. 514

For the digital forensic analyst, an opportunity to acquire or crack the password and decrypt the information may have significant time constraints. Sherwinter[559] highlights that finding the correct encryption key to decrypt encrypted data can take upwards of 2 billion years utilising technology, which at the time of writing in 2007 was standard. Since then, despite computing power improving, encryption standards have increased leaving a similar problem. Part III of RIPA is of particular interest given these developments in computing technology and determining whether a suspect is in possession of illicit material. A brief synopsis of Part III, specifically section 49 RIPA provides public authorities with the power to compel the disclosure of any encryption keys where it is believed the suspect is in possession of such a key. In simple terms, this part of RIPA addresses the issues of obligatory decryption of data[560].

Section 49(2) RIPA allows a public authority to issue a notice of compliance to disclose the encryption key where there is reasonable grounds to believe that a key to the protected information is in the possession of any person. Section 53(5) RIPA states failure to comply can result in a two-year prison sentence or in cases of IDCSA, five years (as introduced by the Policing and Crime Act 2009). This section of RIPA raises a number of questions to address.

First, what are reasonable grounds for believing a suspect is in possession of the key and in turn what should happen if it is forgotten and how could this be proved? Further, encryption is designed to obfuscate data, leaving no indication of what is contained upon the device. Therefore how can a successful prosecution under RIPA stand for possession of images when there is actually little or no physical evidence of the existence of images on an encrypted device in order to prove they are possessed? These are fundamental issues as it seemingly controversial to prosecution a defendant for non-disclosure of an encryption key for suspected child offences without actually confirming the existence of this material. Most likely this will involve some form of interception of communications, lawful surveillance (a power governed by Part II of RIPA) or cyber stings to suggest the presence of illegal material on the encrypted system.

[559] D. J. Sherwinter, 'Surveillance's Slippery Slope: Using Encryption to Recapture Privacy Rights.' (2006) 5 J. on Telecomm. & High Tech. L. 514

[560] B. M. Palfreyman, ' Lessons from the British and American Approaches to Compelled Decryption.' (2009) 75 Brook. L. Rev. 363

Further, it leaves defendants vulnerable to prosecution when they have genuinely forgotten their decryption password, which is arguably impossible to prove. Comments in *S*[561] provide an insight into the reasoning behind password disclosure.

> In this sense the key to the computer equipment is no different to the key to a locked drawer. The contents of the drawer exist independently of the suspect: so does the key to it. The contents may or may not be incriminating: the key is neutral. In the present cases the prosecution is in possession of the drawer: it cannot however gain access to the contents. The lock cannot be broken or picked, and the drawer itself cannot be damaged without destroying the contents.

The reasoning behind requiring password disclosure is to control the usage of encryption techniques and the problems it can pose, limiting the contexts in which it can be used[562], and in some cases providing a deterrent for its criminal use. Palfreyman suggests that the UK has gone too far and infringed upon a the civil liberties of an individual by compelling disclosure in comparison to the protection offer to US citizens and the privilege against self incriminations[563]. Yet without RIPA, the UK is arguably without sufficient measures to fight crime and prevent offending behaviour due to the risk posed by encryption[564].

As a final point, it is necessary to consider whether prosecution under RIPA is a more favourable option for suspects as opposed to disclosing the key and in turn any evidence which may be in existence. The new five-year sentence for under RIPA[565] is the same maximum sentence for the possession of indecent images, however in cases of creation and distribution (an offence attracting a maximum of 10 years under *PCA78*), suspects may be inclined to refuse disclosure where evidence of these crimes may be present in preference for the non-disclosure sentence.

5.6 Concluding Thoughts

The current application of the test of possession set out in *Porter*[566] is not straightforward when applied in the context of digital evidence. Although in theory, the test appears logical in its application, in practice, the shortcomings of digital evidence have led to some

[561] *R v S, A*[2009] 1 Cr. App. R. 18
[562] S. Mason, 'Some international developments in electronic evidence' (2012) Computer and Telecommunications Law Review 23, 30
[563] B. M. Palfreyman, ' Lessons from the British and American Approaches to Compelled Decryption.' (2009) 75 Brook. L. Rev. 363
[564] B. M. Palfreyman, ' Lessons from the British and American Approaches to Compelled Decryption.' (2009) 75 Brook. L. Rev. 363
[565] Regulation of Investigatory Powers Act 2000 s 53
[566] *Porter* [2006] EWCA Crim 560; [2006] 2 Cr. App. R. 25

concerns. In regards to deleted IDCSA, the lack of availability of digital evidence, which could be used to impart knowledge, custody and control of files onto a suspect, has led to difficulties. Further, in relation to the Internet cache, there is now an overlap between the offence of possession and making. Despite the significant difference in their severity, this appears to have arisen as a means of facilitating prosecutions by avoiding the difficulty of having establishing the suspect's knowledge of the cache. Finally encryption now poses a tangible threat to the possession offence, where if implemented effectively, it proves a bar against establishing what content a defendant actually possesses due to limits in decryption powers.

It is also necessary to draw attention to the limitations of Chapter 5. Discussion has focused on fundamental computing technology and its functionality (basic OS, file system and deleted files). Yet, the diverse range of technologies available has meant that it was not possible to include an in-depth analysis of additional systems such as mobile platforms, and is an area of further research. Despite this, the fundamental functionality of file deletion and Internet browser cache discussed in Chapter 5 can be accurately applied to mobile devices with discussion and proposals applicable to both device types.

Chapter 6 provides concluding thoughts on this area of law whilst offering a discussion on potential reforms surrounding the current possession test and a discussion around the development of an additional fifth offence of 'accessing'.

Chapter 6

Conclusions and Considerations for Reform

6.1 Introduction

Throughout this thesis, arguments for the regulation of IDCSA and possession of it have been made citing harm to both the child and to society as founding motivations. By regulating the possession of IDCSA, the demand for IDCSA is arguably stemmed and reduced; those seeking to engage in the material are deterred from doing so, or punished for doing so, and the harm to children involved in creating the illegal imagery is potentially prevented. In turn, effective regulation prevents the normalisation of IDCSA ensuring that the harm it causes continues to be recognised and not tolerated by society. What is key to note is the reactive nature of IDCSA legislation and the constant battle it faces in attempting to promptly address developments in technology which have facilitated those who seek to possess IDCSA. The possession offence is now predominantly a digital offence, where establishing possession of digital files is not straight forward, as highlighted in Chapter 4. These issues were elaborated on in Chapter 5, where problem areas of deleted files, the Internet cache and encryption in relation to establishing an offence of possession of IDCSA have been identified. From the analysis presented in these previous chapters, Chapter 6 provides some concluding thoughts on legislative reforms surrounding the possession of IDCSA offence,

When distilled, this chapter proposes three key areas in relation to potential reforms surrounding IDCSA legislation in England and Wales provided. These areas include the following:

1. Revision of the current approach to cached IDCSA as in *R v Jayson*[567], clarifying the distinction between making and possession.
2. Consider files that have been generated as the result of an intentional act as in possession.
3. Increasing the range of offences to incorporate 'accessing', capturing those who utilise forms of technology like private browsing or streaming, which may inhibit prosecution for possession.

[567] *R. v Smith (Graham Westgarth)* [2003] 1 Cr. App. R. 13 at 33

6.2 Reform 1: Clarify the Distinction Between Making and Possession

As discussed in Chapter 4, possession of IDCSA requires the application of the possession test, as presented in the case of *Porter*[568]. When distilled, possession requires the defendant to maintain the elements of custody and control over the IDCSA in question as well as having knowledge of it. The fundamental problem with the test of possession is that it requires juries to subjectively assess the defendant and whether they possess the requisite knowledge needed to establish possession. This aspect of the possession test can create ambiguity (as in many offences), as there is no defined method for establishing knowledge. In doing so, the offence of possession fails to take into account evidence of intention to possess, which is a position adopted currently by the offence of making IDCSA (discussed in Chapter 5). In essence, the possession and making offences are distinguished by evidence highlighting a suspect's intentions with regards to any IDCSA in question. As a result it is argued that a clearer distinction needs to be drawn between the current making and possession offences to add clarity to this area of law.

6.2.1 Why should the Cache be Possessed?

As with any test which relies on subjective analysis, an element of unreliability remains. This was acknowledged in the case of *R v Jayson*[569], prompting developments in the making offence to compensate for the troublesome application of the possession test, which required the jury to assess the defendant's knowledge of the cache itself. The developments in *R v Jayson*[570] provided an opportunity for law enforcement to prosecute individuals for an offence of making where IDCSA existed in the Internet cache if evidence of intention was present (for example, evidence of searching online for IDCSA). This ruling negated the difficulties related to raising a charge of possession and the need to assess whether the defendant had knowledge of any cached images. Where the possession offence requires evidence of knowledge, the making offence requires establishing evidence of intention, which is arguably easier to achieve (again, evidence of intentional web browsing).

Yet it is argued that the current application of the making offence in regards to the cache is more akin to an act of possession. To highlight this reasoning, an example is provided involving IDCSA found in the Internet cache. Where a defendant is found to have IDCSA within their Internet cache, to raise a charge of possession, the prosecution must be confident of establishing that the defendant has knowledge of the Internet cache and its

[568] *Porter* [2006] EWCA Crim 560; [2006] 2 Cr. App. R. 25
[569] *R. v Smith (Graham Westgarth)* [2003] 1 Cr. App. R. 13 at 33
[570] *R. v Smith (Graham Westgarth)* [2003] 1 Cr. App. R. 13 at 33

functionality. Given the subjective nature of this process and potential unreliability, it is difficult to establish. Yet if evidence of intentional searching of the Internet for IDCSA exists, a making charge can be raised instead, where for the offence of making, there is no requirement to establish knowledge of the cache. In both cases, the creation of the cached images is fundamentally the same, with the only difference being whether a suspect has left evidence of intending to find the images online.

In theory, there appears to be no issue, yet once the functionality of the cache is analysed it is suggested that this decision has left the current law in arguably an unsatisfactory state, where distinction between possessing and making a file appears to hinge solely on evidence of intentional searching. To provide additional explanation, the functionality of the cache must be re-stated. The cache is an automated process designed to improve user performance and experience when browsing the web. The important feature to reiterate is it is automated, and functions without user control. Therefore, despite the fact a user may intentionally visit a website, it is not accurate to suggest they are intentionally caching (and ultimately making) the files from that website to their device and making these files. Instead, the user is simply utilising the functionality of the browser as it was designed (to render web content viewable to the user), and is subject to the functionality of the application itself. In considering cached IDCSA as making (where evidence of searching exists), legally it is considered the same as if a user were to intentionally view an IDCSA online and intentionally save if to their device, possibly for later viewing. Yet the distinction between these two acts is clear, with the later maintaining a greater level of intention. Evidence of intention to search for IDCSA online is not the same as intending to download and possess it (consider someone who solely wants to view content online) and a distinction between these acts should be drawn. At this point, it is suggested that it is more appropriate to treat a defendant as having possession of the IDCSA in their cache. To justify this stance, the fundamental act of making must be examined.

An act of making something requires an intention to make it, i.e. a deliberate want to create that entity. Yet it becomes artificial to suggest that the user has made the content of their cache, which is generated automatically as the result of a separate act (accessing a website, not a intention to create cached files) without user control or subsequent intent, as it is a computer function designed to improve a user's experience when browsing the Internet. It is therefore argued that it is more appropriate to place cached images in the possession of a defendant. This allows for a distinction to be made between IDCSA made by acts of

intentional creation (coined in this thesis as actual-making, such as deliberately downloading and storing an image) and those created as the result of an automated computer function. The overarching complexity existing here lies with the involvement of automated computational processes and the level of culpability that should be attributed to the results of such processes.

Therefore the proposed 1st reform is to readdress the current precedent for cached IDCSA. Where evidence of intentional searching for IDCSA is found, it is argued that cached data should be inferred as in the possession of the suspect, not the product of making. In doing so, a clearer distinction between possessing and making IDCSA is made in relation to the Internet cache. It also ensures that a making offence can be saved for cases involving the actual creation of IDCSA through deliberate acts (creating an image as opposed to one being automatically created as the result of an automated process), as opposed to using the offence to plug the holes left by the current possession test (for example, where a user actually downloads IDCSA from online). This area provides a difficult area of debate, which has arguably lead to the stretching of the current making definition to cover those who are interacting with IDCSA online but may have escaped prosecution under the current possession test. The points raised here give rise to broader debates surrounding issues such as the link between viewing and making and the problems caused by passive browsing online and subsequent evidence left behind by these acts. However, these points remain part of future work beyond this current thesis coverage.

This option for reform still provides an issue, albeit it that it would appear to be overriding the current possession test which requires the element of knowledge and replacing it with intent. This leads to the second proposed reform.

6.3 Reform 2: Considering Evidence of Intentional Acts for Establishing Possession

Digital data and its intangible form coupled with the sheer volume of data that can be stored on a computer system means that establishing possession via establishing knowledge can be difficult. It is not accurate to say that a user 'knows' of all the files on their system, yet it is arguably viable to attribute culpability to files that are of a result of intentional acts carried out on a system by a user. Given the complexity of operating systems, there are potentially an unlimited number of ways that files could be present on a system, beyond the knowledge of the user. Therefore it is argued that a user only possesses those files that they intentionally create or that are created by an intentional act, including those, which stem

from an intentionally run process rather than just those that they directly know about. In doing so, digital forensic analysis of a computer system's activity logs can establish those files which are present due to intentional acts.

The following proposal is offered as an amendment to the current possession test, one that replaces the requirement of knowledge for that of intention.

> (1) A picture is in possession if it has been generated or acquired via a user-initiated process that was activated intentionally.

The motivation behind this comes from the way in which computer systems function coupled with the types of DF evidence, which can support notions of possession. Consider the scenario of IDCSA located in the ThumbCache. The ThumbCache is an OS created file, which remains hidden from the user. It keeps a record of all images that have been stored in folders on a users computer where the Thumbnail view has been used to look at files. As a result, the ThumbCache has a record of images that were stored on the computer, even after the original images have been deleted. Information in the ThumbCache may show that a user has stored and viewed multiple IDCSA in folders on their computer, yet may have since deleted them. As the ThumbCache is likely unknown to the typical computer user, knowledge of it cannot be inferred and therefore neither can possession of its contents. Yet these IDCSA can be present in the ThumbCache as a result of the user intentionally storing and viewing the IDCSA in Thumbnail view in folders on their computer. Therefore the proposed possession definition places IDCSA in the possession of a defendant where they are present on their computer system as a result of their intentional acts. By taking this approach, the difficulty of establishing a defendant's knowledge is negated in favour of evidence of intention that can be determined from expert evidence and an understanding of the functionality of these devices.

6.4 Reform 3: Introduction of a New Offence - Accessing

The final suggested reform is the implementation of a fifth offence, one of accessing. One of the key challenges posed by the Internet and its associated services is that users now have the ability to view IDCSA online but never possess it (given the current legal definition of possession). To provide an example, techniques such as in-private browsing and online streaming (see below for a technical discussion of these concepts) are designed to allow users to access content online without the need to download and store it. As a result, those who access IDCSA online via in-private browsing sessions or streaming are less likely to have

IDCSA downloaded to their PC. Under the range of offences stated in the PCA78 and CJA88, to prosecute, evidence of the IDCSA must first be present in order to then potentially determine which offence has been committed. Those who stream or access content online via private browsing services are likely to have no images downloaded onto their device, yet an offender has still viewed the IDCSA. It is argued that such activities should be punished as although physical possession has not taken place, the defendant has still arguably acquired sexual gratification from viewing the content depicted in the IDCSA. In addition, support for this stance is provided in Chapter 1 where it was identified that further views of IDCSA stand to cause further harm and embarrassment to a child victim. To provide further clarity, Section 6.4.1 will explain how Private Browsing works in practice.

6.4.1 An Example: How Private Browsing Works

Private browsing is increasing in popularity and with the market dominated by both Google Chrome and Mozilla's Firefox browsers[571], both have private browsing functionalities. Private browsing is a relatively recent addition to Internet browser applications as many users seek to privatise their actions whilst browsing online and limit the amount of information regarding their browsing sessions being stored on their local device. Although different Internet browsers implement their private browsing functionality differently, the aim is still the same; to prevent information being retained regarding what they have done online. This often means that any subsequent forensic investigation of a private browsing session is likely to recover a lot less data than if a standard browsing session had been carried out[572]. Records of search history, online website addresses and cached content are often not found on the system (some remnants may be discovered in unallocated areas of a system), with some data left behind in in physical memory (a form of volatile memory used by all computers where content is purged every time the power is removed to the device – i.e. when it is shut down).

The result of these sessions means that despite accessing a website hosting IDCSA online, finding data stored locally on a suspect machine during a forensic investigation indicating this act may not be possible. As a result, we have a scenario where a defendant has accessed

[571] W3Schools, 'Browser Statistics' (W3Schools, 2014) <http://www.w3schools.com/browsers/browsers_stats.asp> accessed 2 May 2014

[572] Magnet Forensics 'How does Chrome's 'incognito' mode affect digital forensics?' (Magnet Forensics, n.d.) <https://www.magnetforensics.com/computer-forensics/how-does-chromes-incognito-mode-affect-digital-forensics/> accessed 2 May 2016

IDCSA and likely obtained sexual gratification from it, an act that is not prohibited within the confines of the current offences surrounding IDCSA.

6.4.2 A Solution: Internet Service Provider Information

After proposing the need for an accessing offence and identifying the problems posed by private browsing, the feasibility of practically implementing this new offence must be discussed. Although at first glance, accessing IDCSA via methods such as private browsing may seem like an act which is difficult to police, there is a solution. Despite private browsing functionalities protecting data from being stored on the defendant's computer, evidence of their visit to an illegal website is maintained by their Internet Service Provider (as confirmed by Google Chromes usage policy[573]). Essentially, private-browsing functionalities implement what can be termed as a 'locally private' service, where information regarding their online actions is not always private from their service provider (BT, SKY etc.). This is particularly important in light of the recent Draft Investigatory Powers Bill.

The Draft Investigatory Powers Bill (DIPB) was presented to the UK Parliament in November 2015 and is designed to replace the Data Retention and Investigatory Powers Act 2014. The UK Parliament states that DIPB "would provide a framework for the use of investigatory powers by law enforcement and security and intelligence agencies, as well as other public authorities. The draft Bill includes provisions for the interception of communications, the retention and acquisition of communications data, the use of equipment interference, and the acquisition of bulk data for analysis"[574]. The focus of DIPB is the regulation of communication untaken by criminals and terrorists and the implementation of powers to intercept, collect and analyse communication traffic. At present, the DIPB is subject to on-going public, academic and industry pre-legislative scrutiny[575], yet has the power to significantly impact law enforcement investigations into criminal behaviour online.

Of particular interest to the facilitation of the offence of accessing proposed in this thesis is the planned communication data collection and retention requirements. To provide insight on what communication data consists of, the DIPB states that "communications data is

[573] Google 'Browse in private with incognito mode' (Google, n.d.) <https://support.google.com/chrome/answer/95464?hl=en-GB> accessed 2 May 2016

[574] Parliament.uk 'Draft Investigatory Powers Bill call for evidence published' <http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-investigatory-powers-bill/news-parliament-2015/call-for-evidence/> accessed 8th March 2016

[575] Joint Committee on the Draft Investigatory Powers Bill 'Draft Investigatory Powers Bill' <http://www.publications.parliament.uk/pa/jt201516/jtselect/jtinvpowers/93/93.pdf> at 1.

information about communications: the 'who', 'where', 'when', 'how' and 'with whom' of a communication but not what was written or said" [576]. One of the main focuses of the DIPB are Internet Connection Records (ICRs). ICRs are records of user's access to online websites and provision which are gathered by ISPs and under the proposed DIPB, ICRs will be maintained by ISPs for up to 12 months. DIPB places the same obligations on all companies providing services to the UK or in control of communications systems in the UK[577]. The DIPB will also clarify the existing powers identified in the Data Retention and Investigatory Powers Act 2014 which is due to expire in December 2016 whilst providing for the retention of communication data for a maximum period of 12 months (see DIPB Part 4, Clause 71).

As the DIPB would seek to record accesses from those who access IDCSA hosting sites, it becomes feasible to implement the following accessing offence.

6.4.3 Implementing an Offence of Accessing

The following statutory amendment is initially proposed to outline the scope of an accessing offence:

> 1) It is an offence for a person to access an indecent photograph [or pseudo-photograph] of a child.
>
> 2) A person accesses an illegal photograph [or pseudo-photograph] if he intentionally accesses a service providing indecent photograph.
>
> 2a) Access shall be determined through Internet connection records
> 2b) Intention shall be established with:
> (i) evidence of direct searching for IDCSA online and;
> (ii) reference to the amount of accesses to IDCSA.
> 2c) A 'service' includes any function allowing access to IDCSA via the Internet

Information for identifying whether a suspect has accessed IDCSA online falls into two scenarios. First, evidence of Internet history on a local device, retrieved during a forensic investigation. This would involve the recovery of Internet history records if they still exist. Second, an analysis of ICRs, tying the browsing records to a suspects IP address. This prevents those who delete the contents of their local device from evading prosecution.

---

[576] Joint Committee on the Draft
Investigatory Powers Bill 'Draft Investigatory Powers Bill'
<http://www.publications.parliament.uk/pa/jt201516/jtselect/jtinvpowers/93/93.pdf> at 12.
[577] Joint Committee on the Draft
Investigatory Powers Bill 'Draft Investigatory Powers Bill'
<http://www.publications.parliament.uk/pa/jt201516/jtselect/jtinvpowers/93/93.pdf> at 30.

Section (2)(b) introduces the need for intention and also makes reference to the use of a service. Note online intentional accesses fall within the confines of the offence, preventing those who are automatically redirected to IDCSA through pop-ups or similar technologies from being prosecuted. Section (2)(b) details how intention is to be inferred, through the support of evidence showing visits have taken place. A key criterion is the amount of accesses, where it would be necessary to establish a threshold of culpability. Steel[578] indicates that there is little evidence of individuals stumbling across IDCSA online and that Internet search engines are commonly used tool to find this type of material. However, consideration of this scenario should be given and ICRs should be taken as a whole to distinguish between those who are actively seeking to access IDCSA online. It is suggested that a threshold of two visits is set. In doing so, mistaken visits are discarded, yet if a defendant returns to the website and continues to access the IDCSA, such actions become prosecutable. This distinguishes between those who stumble across the content and never return and those who go back to view again. As a result, the defendant's course of conduct is considered when establishing whether they have 'accessed' IDCSA under the proposed offence.

The accessing offence can therefore be seen as a method for expanding current legislative powers in terms of apprehending those engaging with IDCSA. It also provides an offence that can be enforced without reliance being placed upon data resident on a suspect's local device, which is subject to being tampered with and destroyed. As accessing can be determined through ICRs stored by ISPs, no longer can an offender rely on technologies which prevent or erase traces of IDCSA from their computing device in order to avoid prosecution. The caveat to this statement lies with the use of provision, which mask the IP address of an offender, such as Tor onion routing protocols. However, despite an increase in the use of this service, the volume of Tor users still remains a substantial less than standard Internet users who are potentially traceable.

6.5 Why expand the range of offences?

The proposal for expanding the existing range of offences to incorporate accessing is driven by developments in technology, which are ultimately facilitating offences surrounding IDCSA. As the law is reactive, it is arguably time for IDCSA legislation to react to provision

[578] C. M. Steel, 'Web-based child pornography: The global impact of deterrence efforts and its consumption on mobile platforms.' (2015) 44 Child abuse & neglect 150

offering access to IDCSA in a way that is currently not within the bounds of existing offences. As computing devices and applications have developed to allow users to covertly access and interact with IDCSA, there is a need to prohibit those who utilise these techniques to carry out this activity. As possession of IDCSA is prohibited for the reasons noted in Chapter 2, it is argued that accessing IDCSA should also be prohibited. Expanding the current range of offences to include accessing can be argued as a being a reactive measure, one that is necessary in order to tackle an existing gap in legislation. Prosecuting accessing also serves as a deterrent as individuals are not only liable for content stored on their local devices but also for their actions online where they have visited illegal websites.

6.6 Final Concluding Thoughts

It is clear that the regulation of IDCSA currently poses one of the greatest challenges to law enforcement and there are no signs of change. With the harm to both the child and society documented, the need to prohibit access to IDCSA is great, despite concerns that we will never truly effectively control and stem the creation of this material. This thesis has highlighted the harms caused to the child and society by IDCSA and the need to regulate this content. A chronological review of the legislative developments surrounding IDCSA was presented, followed by an analysis of the concept of possession. Key areas of difficulty with regards to regulating IDCSA have been presented, including the Internet cache, deleted content and encryption. Finally potential legislative reforms have been offered.

Bibliography

A Staff Reporter, ‘Mrs Thatcher urges action over child pornography.’ *Times* (London, 6 September 1977) accessed 28 February 2015.

Adobe, 'Photoshop CC' (www.adobe.com 2013) <http://www.adobe.com/uk/products/photoshop.html> accessed 19 December 2013

Akdeniz, Y., 'The regulation of pornography and child pornography on the Internet' (1997) The Journal of Information, Law and Technology 1, 1

Akdeniz, Y., ‘Case report: Court of Appeal clarifies the law on downloading pornography from the Web.’ (2002) 18.6 Computer Law & Security Review 433

Akdeniz, Y., 'Possession and dispossession: a critical assessment of defences in possession of indecent photographs of children cases' [2007] Crim. L.R. 274, 280

Akdeniz, Y., *Internet Child Pornography and the Law: National and International Responses* (1st, Ashgate Publishing 2013) 326

Alderson, K., ‘Businessman, 48, collected child porn from Internet.’ *Times* (London, 27 October 1995) accessed 12 February 2015

Allsop, K., ‘The row about Lolita.’ *Daily Mail* (London, 18 December 1958) accessed 21 February 2015

Anon ‘Obscene books Bill gets reading.’ *Daily Mail* (London, 19 November 1958) accessed 21 February 2015 and Anon ‘Changes Proposed In Law On Obscene Publications.’ *Times* (London, 28 March 1958) accessed 21 February 2015

Anon ‘Changes Proposed In Law On Obscene Publications.’ *Times* (London, 28 March 1958) accessed 28 February 2015

Anon, ‘Author Says Novel 'Fanny Hill' Not Pornography.’ *Times* (London, 21 January 1964) accessed 21 February 2015.

Anon, ‘’Jail filth tycoons'.’ *Daily Mail* (London, 4 February 1964) accessed 21 February 2015.

Anon ‘Scotland Yard Looks Into Mail Order Pornography.’ *Times* (London, 2 September 1964) accessed 21 February 2015.

Anon ‘Mr Rees willing to see if law can be tightened to tackle child pornography.’ *Times* (London, 18 November 1977) accessed 12 February 2015.

Anon ‘Bill to control child pornography makes the law more effective.’ *Times* (London, 6 May 1978) accessed 12 February 2015.

Anon, ‘Second reading for Bill to curb child pornography: Tory MP speaks of growing public anxiety.’ *Times* (London, 11 February 1978) accessed 28 February 2015

Anon ‘Bill to control child pornography makes the law more effective.’ *Times* (London, 6 May 1978) accessed 12 February 2015.

Anon, ‘PIE member faces child pornography charge.’ *Times* (London, 17 November 1984) accessed 21 February 2015.

Anon ‘Child porn nurse sent to jail.’ *Daily Mail* (London, 21 August 1986) accessed 21 February 2015.

Anon, ‘Gary Glitter 'in child porn probe'.’ *Times* (London, 19 November 1997) accessed 12 Feb. 2015.

Anon, 'Timeline: The Sarah Payne tragedy' *BBC News* (London, 12 December 2001) <http://news.bbc.co.uk/1/hi/england/1703534.stm> accessed 8 February 2014

Anon, 'Ex-paedophile group leader Freeman jailed over child rape drawings' *BBC News* (London, 15 July 2011) <http://www.bbc.co.uk/news/uk-england-london-14169406> accessed 16 January 2015

Anon, 'Lostprophets' Ian Watkins sentenced to 35 years over child sex offences' *BBC News* (18 December 2013) <http://www.bbc.co.uk/news/uk-wales-25412675> accessed 1 September 2014

Anon 'Crimes Against Children' COM/FS/2013-10/THB-03 (Interpol 2013) <www.interpol.int/content/download/19248/170122/version/15/file/Factsheets_EN_oct2013_THB03%20web.pdf> accessed 15 June 2014

Anon, 'About the CEOP Centre' *CEOP* (Child Exploitation and Online Protection Centre 2013) <http://ceop.police.uk/About-Us/> accessed 24 August 2013

Anon, 'At A Glance' *INHOPE* (INHOPE n.d.) <http://www.inhope.org/gns/who-we-are/at-a-glance.aspx> accessed 19 March 2014

Antoniou, A., 'Possession of prohibited images of children: three years on' (2013) 77.4 J. Crim. L. 337, 338

Aries, P., *Centuries of Childhood* (1st, Penguin 1962) 125

Bailey, J., 'Confronting Collective Harm: Technology's Transformative Impact on Child Pornography' (2007) 56 U.N.B.L.J. 65, 67

Barratt, M. J., S. Lenton & M. Allen, 'Internet content regulation, public drug websites and the growth in hidden Internet services.' (2013) 20.3 Drugs: education, prevention and policy 195

Basta, A., N. Basta, & M. Brown, *Computer Security and Penetration Testing* (1st, Cengage Learning 2013) 64

Bell, R. E., 'The prosecution of computer crime' (2002) 9.4 J.F.C. 308

Betts, G., 'Powers of Criminal Courts (Sentencing) Act 2000: Committal for Sentencing.' (2012) 76 J. Crim. L. 12

Bovey, K. S., 'Possession revisited' (2005) S.L.T. 475, 475

Burke, D. D., 'The Criminalization of Virtual Child Pornography: A Constitutional Question' (1997) 34 Harv. J. on Legis. 439

Burke, A., S. Sowerbutts, S. Blundell & M. Sherry, 'Child pornography and the internet: Policing and treatment issues.' (2001) 9.1 Psychiatry, Psychology and Law 79

Butt, R., 'Stamp it out, this abominable evil of using children for pornography.' *Times* (London, 24 November 1977) accessed 12 February 2015.

Calder, M., 'The internet: Potential, problems and pathways to hands-on sexual offending' (2004) In M. Calder (Ed.) Child sexual abuse and the internet: Tackling the new frontier 2 (Russell House Publishing Ltd)

Carr, J. *Child abuse, child pornography and the Internet* (1st, NCH 2003)

Carr, J. & Z. Hilton, 'Combatting Child Abuse Images on the Internet' in J. Davidson & P. Gottschalk (eds), *Internet Child Abuse Current Research and Policy* (1st, Routledge 2011)

Casey, E., *Handbook of Digital Forensics and Investigation* (1st, Academic Press 2009)

Casey, E., *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd, Academic Press 2011)

Cassell, P. G., J. R. Marsh & J. M. Christiansen, 'Case for Full Restitution for Child Pornography Victims, The.' (2013) 82 Geo. Wash. L. Rev. 61.

CEOP, Annual Review 2012-2013 & Centre Plan (2013), pg.7

CEOP, 'Threat Assessment of Child Sexual Exploitation and Abuse' (2013) 8 < https://ceop.police.uk/Documents/ceopdocs/CEOP_TACSEA2013_240613%20FINAL.pdf > accessed 6 December 2015

Chatterjee, B. B., 'New but not improved: a critical examination of revisions to the Regulation of Investigatory Powers Act 2000 encryption provisions' (2011) 19.3 Int J Law Info Tech 264

Cheng, Y. E., 'Pornography: women matter' (2002) UCL Jurisprudence Review 144, 145

Chock, P. N., 'The Use of Computers in the Sexual Exploitation of Children and Child Pornography' (1987) 7.3 Computer/L.J. 383, 392

Clark, G., Political Correspondent, 'Tory call to strengthen law on child pornography.' *Times* (London, 15 November 1977) accessed 12 February 2015

Clough, J., 'Now you see it, now you don't: digital images and the meaning of 'possession'' (2008) 19 Criminal Law Forum 205

Clough, J. 'Lawful Acts, Unlawful Images: The Problematic Definition of Child Pornography' (2012) 38 Monash U. L. Rev. 213

Cohen-Almagor, R., 'Online Child Sex Offenders: Challenges and Counter-Measures.' (2013) 52.2 The Howard Journal of Criminal Justice 190

Coleman, C. 'Jury age limit to be raised to 75 in England and Wales' *BBC News* (BBC News, 20 August 2013) <http://www.bbc.co.uk/news/uk-23764925?utm_source=dlvr.it&utm_medium=twitter> accessed 20 August 2013

Conley, P. C., 'Behind Closed Doors-The Clandestine Problem of Child Pornography.' (1987) 21 Creighton L. Rev. 917

Corby, B., *Child Abuse Towards a Knowledge Base* (1st, Open University Press 1993)

CPS, 'Indecent photographs of children' <http://www.cps.gov.uk/legal/h_to_k/indecent_photographs_of_children/> accessed 14 May 2015

CPS, *'Violence against Women and Girls Crime Report' (2015) <http://www.cps.gov.uk/publications/docs/cps_vawg_report_2015_amended_september_2015_v2.pdf> accessed 30 November 2015*

Crystal, D., *Language and the Internet* (1st, Cambridge University Press, 2001)

Culture, Media and Sport Committee, Online Safety (HC 2013, 125-222) available at <http://www.publications.parliament.uk/pa/cm201314/cmselect/cmcumeds/729/729.pdf> accessed 16 January 2016

Daniel, L. E., *Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom* (1st, Elsevier 2011) 62

Davidson, J. & P. Gottschalk, *Internet Child Abuse Current Research and Policy* (1st, Routledge 2011) 197

Davidson, J., J. Grove-Hills, A. Bifulco, P. Gottschalk, V. Caretti, T. Pham, & S. Webster, 'Online abuse: literature review and policy context' (2011) European Online Grooming

Project <http://www.scotcen.org.uk/media/22523/european-online-grooming-projectliteraturereview.pdf> accessed 14 June 2016

Davidson, J., M. Lorenz, E. Martellozzo, & J. Grove-Hills, *Evaluation of CEOP Think U Know Internet Safety Programme and Exploration of Young People's Internet Safety Knowledge* (1st, 2010)

De Mause, L., *The History of Childhood* (1st, Souvenir Press 1976)

Diez, E. R., 'One Click, You're Guilty: A Troubling Precedent for Internet Child Pornography and the Fourth Amendment' (2006) 55 Cath. U. L. Rev. 759

Dingledine, R., N. Mathewson & P. Syverson, 'Tor: The second-generation onion router' (2004) Naval Research Lab Washington DC 1, 1
Edwards, S. S. M., 'A safe haven for hardest core' (1997) 8 Ent. L.R. 137

Doherty, E. P. *Digital Forensics for Handheld Devices* (1st, CRC Press 2012) 41

D'Orlando, F., 'The demand for pornography' (2011) 12 Journal of Happiness Studies 51

Easton, S., *The Problem of Pornography: Regulation and the Right to Free Speech* (1st, Routledge 2005) 132

Easton, S., 'Criminalising the Possession of Extreme Pornography: Sword or Shield?' (2011) 75 JCL 391

Edwards, L., & C. Waelde, *Law and the Internet* (3rd, Hart Publishing 2009) 632

Elliott, I. A., & A. R. Beech, 'Understanding online child pornography use: Applying sexual offense theory to internet offenders.' (2009) 14.3 Aggression and Violent Behavior 180

Elman, R. A., *Sexual Politics and the European Union: The New Feminist Challenge* (1st, Berghahn Books, 1996) 73

Endrass, J., F. Urbaniok, L. C. Hammermeister, C. Benz, T. Elbert, A. Laubacher & A. Rossegger, 'The consumption of Internet child pornography and violent and sex offending.' (2009) 9.1 BmC Psychiatry 43

Exum, J. J., 'Making the Punishment Fit the (Computer) Crime: Rebooting Notions of Possession for the Federal Sentencing of Child Pornography Offenses.' (2009) 16 Rich. JL & Tech. 16 1, 32

Fenwick, H., *Civil Liberties and Human Rights* (4th, Routledge 2009) 583

Fineman, M., *Faking it: Manipulated Photography Before Photoshop* (1st, Metropolitan Museum of Art 2012)

Fontaine, J. L., *Child Sexual Abuse* (1st, Polity Press 1990) 108

Foreman, J., 'Can We End the Shame?--Recent Multilateral Efforts to Address the World Child Pornography Market' (1990) 23 Vand. J. Transnat'l L. 435, 438

Fortson, R., 'R. v Williams (Orette): burden of proof - firearms offence' (2013) Crim. L.R. 983, 985

Gant, K., 'Crying over the Cache: Why Technology has Compromised the Uniform Application of Child Pornography Laws' (2012) 81 Fordham L. Rev. 319, 319

Gibbons, T., 'Computer generated pornography' [1995] International Review of Law, Computers & Technology 85, 85.

Gilbert, J., 'Computer bulletin board operator liability for user misuse.' (1985) 54 Fordham L. Rev. 439

Gillespie, A. A., 'Child pornography: balancing substantive and evidential law to safeguard children effectively from abuse' (2005) 9.1 International Journal of Evidence & Proof 29, 49

Gillespie, A. A., 'Defining Child Pornography: Challenges for the Law' (2010) 22 Child & Fam. L. Q. 200, 201

Gillespie, A. A. 'Incitement to distribute indecent photographs of children revisited' (2011) 75.3 J. Crim. L. 168, 168

Gobert, J. J., 'The peremptory challenge - an obituary' [1989] Crim. L.R. 528

Google 'Browse in private with incognito mode' (Google, n.d.) <https://support.google.com/chrome/answer/95464?hl=en-GB> accessed 2 May 2016

Green, S., 'The subject matter of conversion' (2010) J.B.L. 218, 221

Griffith, J. D., T. M. Libkuman & D. A. Poole, 'Repressed memories: The effects of expert testimony on mock jurors' decision making.' (1998) American Journal of Forensic Psychology

Harrison, J., 'Whitelaw urges child porn blitz.' *Daily Mail* (London, 15 November 1977) accessed 28 February 2015

HC Deb 17th November 1977, Vol 939, col 737-978

HC Deb 10 February 1978,vol 943, col 1832-744

HC Deb 14 July 1978, Vol 953, col 1919-848

HC Deb 27 June 1984 vol 62 cc1014-6.

HC Deb 29 November 1985 vol 87, col 1117-718

HC Deb 22 December 1988 vol 144 cc426-7W

HC Deb 28 June 1988 vol 136, col 177-344

HC Deb 18 December 2001 vol 377 cc251-2W

HC Deb 08 May 2002 vol 385 c233W

HC Deb, 12th June 2013, vol 564, col 383

HC Deb, 12th June 2013, vol 564, col 396

HC Deb, 12th June 2013, vol 564, col 397

HC Deb, 12th June 2013, vol 564, col 399

HC Deb, 4th July 2013, vol 565, col 1142

Heffer, S., 'Don't Let Them Slip the Net.' *Daily Mail* (London, 5 September 1998) accessed 2 March 2015.

Hessick, C. B., 'Disentangling child pornography from child sex abuse.' (2010) 88 Wash. UL Rev. 853

Hessick, C. B., 'The Limits of Child Pornography' (2014) 89 Ind. LJ 1437

HL Deb 5 May 1978, vol 391, col 527-670

HL Deb 25 March 1982 vol 428 cc1083-130

HL Deb 15 May 1984 vol 451 c1397WA

HL Deb 17 March 1988 vol 494 cc1251-3

HL Deb 22 July 1988 vol, 499 col, 1583-1710

HL Deb 04 October 2000 vol 616 cc1564-89

HL Deb 4 October 2000 vol 616, col 1509-1680

Holmes, S. T. & R. M. Holmes, *Sex Crimes Patterns and Behaviours* (1st, Sage Publications 2002) 291

Home Office and Scottish Executive, *'Consultation: On the Possession of Extreme Pornographic Material'* (2005) 1

Home Office, *Consultation on Possession of Non-photographic Visual Depictions of Child Sexual Abuse* (Home Office, 2007) <http://www.scotland.gov.uk/Resource/Doc/1099/0048474.pdf> accessed 15 January 2016

Horsman, G., 'The challenges surrounding the regulation of anonymous communication provision in the United Kingdom.' (2016) 56 Computers & Security 151

Houtepen, J., J. J. Sijtsema & S. Bogaerts, 'From child pornography offending to child sexual abuse: A review of child pornography offender characteristics and risks for cross-over.' (2014) 19.5 Aggression and violent behavior 466

Howard, T. E., 'Don't Cache out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files' (2004) 9 Berkeley Tech. L.J. 1255

INHOPE, '*Annual Report 2012' (2012) 13*

Internet Watch Foundation, 'About Us' (IWF, n.d.) <https://www.iwf.org.uk/about-iwf> accessed 14 May 2015

Internet watch foundation, 'IWF announce record reports of child sexual abuse online' (*Iwforguk*, 7 May 2016) <https://www.iwf.org.uk/about-iwf/news/post/444-iwf-announce-record-reports-of-child-sexual-abuse-online> accessed 7 May 2016

Interpol, 'Appropriate Terminology' (Interpol, n.d.) <http://www.interpol.int/Crime-areas/Crimes-against-children/Appropriate-terminology> accessed 2015 November 2

IWF*, 'R V Bowden' (iwf.org, n.d.) <https://www.iwf.org.uk/hotline/case-laws/r-v-bowden> accessed 10 January 2015*

IWF, 'R v Freeman' (iwf.org, n.d.) <https://www.iwf.org.uk/hotline/case-laws/r-v--freeman> accessed 16 January 2015

Ivezaj, G., 'Child Pornography on the Internet: An Examination of the International Communities Proposed Solutions for a Global Problem' (1999) 8 Mich. St. U.-DCL J. Int'l L. 819, 823

Jauron, J., 'Paperless Pornography' (1994) 1 EDI L. Rev. 163, 166

Jenkins, P., *Beyond Tolerance: Child Pornography on the Internet* (1st, NYU Press 2003)

Jewkes, Y., & C. Andrews, *Internet Child Pornography: International Responses* in Willian (eds), *Crime Online* (1st, Willan Publishing 2007)

Johnson, D. B., 'Why the Possession of Computer-Generated Child Pornography Can Be Constitutionally Prohibited' (1994) 4 Alb. L.J. Sci. & Tech. 311, 312

Johnson, M. & K. M. Rogers, 'Too Far Down the Yellow Brick Road - Cyber-Hysteria and Virtual Porn' (2009) 4 J. Int'l Com. L. & Tech. 61, 61

Jones, A., & C. Valli, *Building a Digital Forensic Laboratory* (1st, Butterworth-Heinemann 2011) 108

Jones, L. M., 'Regulating Child Pornography on the Internet - The Implications of Article 34 of the United Nations Convention on the Rights of the Child' (1998) 6 Int'l J. Child. Rts. 55, 57

Juels, A., M. Jakobsson & T. N. Jagatic 'Cache cookies for browser authentication.' In *Security and Privacy, 2006 IEEE Symposium* on 2006 May 21, 5

Kendrick, W. M., *The Secret Museum: Pornography in Modern Culture* (1st, University of California Press 1987) 318

Kleinhans, M. M., 'Criminal justice approaches to paedophilic sex offenders.' (2002) 11.2 Social & Legal Studies 233, 233

Kortlander, J., 'Is filtering the new silver bullet in the fight against child pornography on the internet? A legal study into the experiences of Australia and Germany' (2011) 17.7 Computer and Telecommunications Law Review 199, 199

Krone, T., 'A typology of online child pornography offending.' (2004) Australian Institute of Criminology

Lambert, N. M., S. Negash, T. F. Stillman, S. B. Olmstead, & F. D. Fincham, 'A love that doesn't last: Pornography consumption and weakened commitment to one's romantic partner' (2012) 31 Journal of Social and Clinical Psychology 410, 410

Lee, A., 'Child pornography videos found at home of Chancellor's adviser.' *Times* (London, 14 January 1997) accessed 27 Feb. 2015.

Lee-Potter, L., 'Depravity on the Internet.' *Daily Mail* (London, 4 September 1998) accessed 21 February 2015

Levy, N., 'Virtual child pornography: The eroticization of inequality.' (2002) 4.4 Ethics and Information Technology 319

Lindgren, J. 'Defining pornography' (1993) 114 University of Pennsylvania Law Review 1153.

Linz, D., E. Donnerstein & S. M. Adams, 'Physiological desensitization and judgments about female victims of violence.' (1989) 15.4 Human Communication Research 509

Losavio, M., 'The law of possession of digital objects: dominion and control issues for digital forensics investigations and prosecutions' (2005) Systematic Approaches to Digital Forensic Engineering 177, 177

Lukas, A., 'Exploring the Extent to Which the Utilization of Technology Has Facilitated the Increased Possession of Online Child Pornography over Time.' (Masters of Science in Criminal Justice thesis, Kennesaw State University 2013)

MacKinnon, C. A., 'Pornography, civil rights, and speech' (1985) 20 Harv. CR-CLL Rev. 1

Magnet Forensics 'How does Chrome's 'incognito' mode affect digital forensics?' (Magnet Forensics, n.d.) <https://www.magnetforensics.com/computer-forensics/how-does-chromes-incognito-mode-affect-digital-forensics/> accessed 2 May 2016

Manchester, C., 'Criminal Justice and Public Order Act 1994: obscenity, pornography and videos' [1995] C. L. R. 123, 123

Manning, R. 'Plugging in to Computer Bulletin Boards.' (1986) ERIC Digest

Marin, G., 'Possession of Child Pornography: Should you be Convicted When the Computer Cache Does the Saving for You' (2008) 60 Fla. L. Rev. 1207

Mason, S., 'Some international developments in electronic evidence' (2012) Computer and Telecommunications Law Review 23, 30

McCaskill, S., 'New National Curriculum To Teach Five Year Olds Computer Programming' (TechWeek, 2013) <http://www.techweekeurope.co.uk/news/national-curriculum-ict-education-computing-121214> accessed 20 August 2013

McGlynn, C., & E. Rackley, 'Criminalising extreme pornography: a lost opportunity' (2009) 4 Criminal law review 245, 246

McGurran, D., 'Cambridge's Internet Watch Foundation leads child abuse clean up' *BBC News* (Norfolk, 20 November 2013) <http://www.bbc.co.uk/news/25005541> accessed 15 March 2014

McIntyre, T. J., 'Blocking child pornography on the Internet: European Union developments' (2010) 24.3 International Review of Law, Computers & Technology 209

Michaels, R., 'Criminal Law-The Insufficiency of Possession in Prohibition of Child Pornography Statutes: Why Viewing a Crime Scene Should Be Criminal.' (2008) 30 W. New Eng. L. Rev. 817, 818

Microsoft, 'What is Encryption?' (Windows, 2014) <http://windows.microsoft.com/en-gb/windows/what-is-encryption#1TC=windows-7> accessed 20 January 2014

Midgley, C., 'Employee 'kept porn library on university computer' *Times* (London, 30 March 1996) accessed 1 March 2015.

Miller, M., *Special Edition Using the Internet and Web* (1st, Que Publishing 2001)

Mills, I. H., 'Effects of child pornography.' *Times* (London, 15 February 1978) accessed 21 February 2015.

Millwood Hargrave, A, & S. Livingstone, *Harm and Offence in Media Content: A Review of the Evidence* (2nd, Intellect Books 2009) 115
Monaghan, N., 'The problem of jury misbehaviour in an internet age: recent cases and the Law Commission's consultation' (2013) 18.1 Cov. L.J. 73

Monterosso, F. S., 'Protecting the Children: Challenges that Result in, and Consequences Resulting from, Inconsistent Prosecution of Child Pornography Cases in a Technical World.' (2009) 16 Rich. JL & Tech. 1

Moon, K., 'The nature of computer programs: tangible? goods? personal property? intellectual property?' (2009) 8 European Intellectual Property Review 396, 398

Moore, D., & T. Rid, 'Cryptopolitik and the Darknet.' (2016) 58.1 Survival 7

Morris, C., 'Porn Industry Feeling Upbeat About 2014' *NBC News* (U.S., 14 January 2014) <http://www.nbcnews.com/business/business-news/porn-industry-feeling-upbeat-about-2014-n9076> accessed 12 September 2014

Nair A., & J. Griffin, 'The regulation of online extreme pornography: purposive teleology (in) action' (2013) 21.4 Int J Law Info Tech 329

Noyes, H., Parliamentary Correspondent, 'Vote not needed on child pornography Bill.' *Times* (London, 11 February 1978) accessed 12 February 2015.

O'Donnell I. & C. Miller, *Child Pornography; Crime, computers and society* (1st, Willan Publishing 2007) 259

Office of National Statistics, *Chapter 4 - Housing and Consumer Durables (General Lifestyle Survey Overview - a report on the 2011 General Lifestyle Survey) (2013) 6*

Office of National Statistics, *Internet Access – Households and Individuals* (2013), 34

Office of National Statistics, 'Internet Access – Households and Individuals: 2015' (*ONS*, 6 August 2015) <http://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2015-08-06#household-internet-access> accessed 22 June 2016

Ormerod, D. C., 'Commentary on *R. v Porter*' [2006] Crim. L.R. 748.

Ormerod, D. C., 'Indecent Photograph of a Child' [2006] *Crim. L. R.* 748, 750.

Ost, S., *Child Pornography and Sexual Grooming: Legal and Societal Responses* (1st, Cambridge University Press 2009) 273

Oswell, D., 'The Place of 'Childhood' in Internet Content Regulation A Case Study of Policy in the UK' (1998) 1.2 International Journal of Cultural Studies 271, 271

OUR CORRESPONDENT, 'Action Urged On Pornography.' *Times* (London, 29 December 1961) accessed 21 February 2015

Oxforddictionaries.com, 'Pornography' (Oxford Dictionaries, n.d.) <http://www.oxforddictionaries.com/definition/english/pornography> accessed 10 January 2016

Oxforddictionaries.com, 'necrophilia' (Oxford Dictionaries, n.d.) <http://www.oxforddictionaries.com/definition/english/necrophilia?q=necrophilia> accessed 9 February 2014

Oxforddictionaries.com, 'snuff movie' (Oxford Dictionaries n.d.) <http://www.oxforddictionaries.com/definition/english/snuff-movie?q=snuff+movie> accessed 9 February 2014

Oxforddictionaries.com, 'Indecent ' (Oxford Dictionaries n.d.) <http://www.oxforddictionaries.com/definition/english/indecent?q=indecent> accessed 15 March 2014

Oxforddictionaries.com, 'Abuse' (Oxford Dictionaries n.d.) <http://www.oxforddictionaries.com/definition/english/abuse> accessed 12 September 2014

Oxford Dictionaries, 'Definition of possession in English ' (Oxford Dictionaries, 2013) <http://oxforddictionaries.com/definition/english/possession?q=possession> accessed 19 August 2013

Oxford Dictionaries, 'intangible' (Oxford Dictionaries, 2014) <http://www.oxforddictionaries.com/definition/english/intangible?q=intangible> accessed 16 February 2014

Oxford Dictionaries, 'tangible' (Oxford Dictionaries, 2014) <http://www.oxforddictionaries.com/definition/english/tangible?q=tangible> accessed 16 February 2014

Palfreyman, B. M., ' Lessons from the British and American Approaches to Compelled Decryption.' (2009) 75 Brook. L. Rev. 363

Peisert, S., M. Bishop & K. Marzullo, 'Computer Forensics In Forensis.' (2008) Proceedings of the Third International IEEE Workshop on Systematic Approaches to Digital Forensic Engineering (IEEESADFE) 102

Phelps A., & A. Watt, 'I shop online–recreationally! Internet anonymity and Silk Road enabling drug use in Australia.' (2014) 11.4 Digital Investigation 261

Piriform, 'CCLeaner - PC Optimization and Cleaning' (CCleaner, 2013) <http://www.piriform.com/ccleaner> accessed 20 August 2013

Prichard, J., C. Spiranovic, P. Watters & C. Lueg, 'Young people, child pornography, and subcultural norms on the Internet.' (2013) 64 Journal of the American Society for Information Science and Technology 992

Quayle, E. & M. Taylor, 'Paedophiles, pornography and the Internet: Assessment issues' (2002) 32.7 British Journal of Social Work 863

Quayle, E., & M. Taylor, 'Child pornography and the Internet: Perpetuating a cycle of abuse.' (2002) 23.4 Deviant Behavior 331

Quayle, E., 'The COPINE project' (2008) 5 Irish Probation Journal 65, 67

Ramirez, J. A., 'Propriety of internet restrictions for sex offenders convicted of possession of child pornography: should we protect their virtual liberty at the expense of the safety of our children?.' (2014) 12 Ave Maria L. Rev. 123

Réka, A., H. Jeong & A. Barabási, 'Internet: Diameter of the world-wide web' (1999) 401 Nature 130, 130

Roberts, P., 'Drug dealing and the presumption of innocence: The Human Rights Act (almost) bites' (2002) 6.1 International Journal of Evidence & Proof 17, 23

Rojas, R, & U. Hashagen, *The First Computers: History and Architectures* (1st, MIT Press 2002) 18

Rose, P., Peter, Chief Crime Correspondent, '100 held in global child-porn swoop.' *Daily Mail* (London, 3 September 1998) accessed 21 February 2015)

Rowbottom, J., 'Obscenity laws and the internet: targeting the supply and demand' (2006) Crim. L.R. 97, 98

Ryder, B.,'The Harms of Child Pornography Law' (2002) 32 U. Brit. Colum. L. Rev. 101, 102

Sammons, J., *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics* (1st, Elsevier 2012)

Samuels, A., 'Obscenity and Pornography' (2009) JPN 187

Scheller, J. C., 'PC Peep Show: Computers, Privacy, and Child Pornography' (1994) 27 J. Marshall L. Rev. 989, 989

Scotford, A., *et al*. 'Now let's have a clean-up on the bookstalls.' *Daily Mail* (London, 18 April 1961) accessed 28 February 2015.

Selfe, D., 'Extreme pornographic images - mens rea and defences' (2011) Crim. Law. 4

Shartel, B., 'Meanings of Possession' (1932) 16 Minn. L. Rev. 611

Sherwinter, D. J., 'Surveillance's Slippery Slope: Using Encryption to Recapture Privacy Rights.' (2006) 5 J. on Telecomm. & High Tech. L. 514

Silbert, M. H., 'On Effects on Juveniles of Being Used for Pornography and Prostitution' (1989), in D. Zillman and C. Bryant, *Pornography: Research Advances and Policy Considerations, (*Hillside, NJ: Lawrence Erlbaum)

Silverman, J., & D. Wilson, *Innocence Betrayed Paedophilia, the Media and Society* (1st, Blackwell Publishing 2002) 2

Smith, L. S., 'Private Possession of Child Pornography: Narrowing at-Home Privacy Rights' [1991] Ann. Surv. Am. L. 1011, 1013

Sommer, P., 'Evidence in Internet paedophilia cases' (2002) 8.7 C.T.L.R. 176

Steel, C. M., 'Web-based child pornography: The global impact of deterrence efforts and its consumption on mobile platforms.' (2015) 44 Child abuse & neglect 150

Stone, R., 'Extending the Labyrinth: Part VII of the Criminal Justice and Public Order Act 1994.' (1995) 58.3 The Modern Law Review 389

Stone, R., *Textbook on Civil Liberties and Human Rights* (10th, Oxford University Press 2014) 355

Strossen, N., *Defending Pornography: Free Speech, Sex, and the Fight for Women's Rights* (1st, NYU Press, 2000) 320

Sullivan, J., & A. Beech, 'Assessing internet offenders' (2004) In M. Calder (Ed.) *Child sexual abuse and the internet: Tackling the new frontier* 69 (UK Russell House Publishing Ltd)

Symon, P., 'Home Office criticized on child pornography.' *Times* (London, 4 February 1978) accessed 21 February 2015.

Symon, P., 'Fears over children lured into pornography.' *Times* (London, 9 February 1978) accessed 28 February 2015.

Tate, T., *Child Pornography: An Investigation* (1st, Methuen 1990)

Taylor, M., 'The nature and Dimension of Child Pornography on the Internet' Paper presented at the international conference 'Combating Child Pornography on the Internet' (1999)

Taylor, M., & Quayle E., *Child pornography: an Internet crime. (*1st, Brunner-Routledge 2003)

Tendler, S., Crime Reporter, 'Computer link used in child pornography.' *Times* (London, 29 July 1987) accessed 21 February 2015.

Thomas, D. S., 'Cyberspace pornography: Problems with enforcement' (1997) 7.3 Internet Research 201

Travis, A., *Bound & Gagged: a Secret History of Obscenity in Britain* (1st, Profile Books 2000) 293

Triggle, N., 'Jimmy Savile NHS abuse victims aged five to 75' *BBC News* (London, 26 June 2014) <http://www.bbc.co.uk/news/uk-28034427> accessed 1 September 2014

United Nations Office on Drugs and Crime 'Comprehensive Study on Cyber Crime' (2013) pg. 26

Vidmar, N., 'Generic Prejudice and the Presumption of Guilt in Sex Abuse Trials' (1997) 21.1 *Law and Human Behaviour* 5

W3Schools, 'Browser Statistics' (W3Schools, 2014) <http://www.w3schools.com/browsers/browsers_stats.asp> accessed 2 May 2014

Walden, I., 'Safeguards in the ether' (2010) European Lawyer 53, 53

Ward, M., 'Do dark networks aid cyberthieves and abusers?' BBC News Technology (20 June 2013) <http://www.bbc.co.uk/news/technology-22754061> accessed 19 January 2014

Ward, M., 'Web porn: Just how much is there?' *BBC News* (London, 1 July 2013) <http://www.bbc.co.uk/news/technology-23030090> accessed 12 September 2014

Webb, L., J. Craissati, & S. Keen, ‘Characteristics of Internet child pornography offenders: A comparison with child molesters.’ (2007) 19.4 Sexual abuse: a journal of research and treatment 449

Wells, M., *et al*. ‘Defining child pornography: Law enforcement dilemmas in investigations of Internet child pornography possession’ (2007) 8.3 Police Practice and Research 269

Wessels, D., *Web Caching* (1st, O'Reilly Media 2001)

Wilkinson, P., & R. Gledhill, ‘Paedophile priest circulated porn on the Internet.’ *Times* (London, 13 November 1996) accessed 12 February 2015)

Williams B. & A. Owen, ‘Report of the committee on obscenity and film censorship’ (1979) 7772 Stationery Office 8.2

Williams, K. S., 'Child-Pornography and Regulation of the Internet in the United Kingdom: The Impact on Fundamental Rights and International Relations' (2002) 41 randeis L.J. 463, 469

Willmore, K., ‘Protecting child victims' rights as vigorously as criminal defendants' when prosecuting possession or distribution of child pornography.’ (2012) 87.3 Washington Law Review 887

Wilson, C., ‘Where can I take Aunt Edna?’ *Daily Mail* (London, 2 November 1959) accessed 21 February 2015

Wolak, J., D. Finkelhor & K. J. Mitchell, *Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study* (Crimes against Children Research Center, 2005)

Wolak, J., K. Mitchell, & D. Finkelhor, ‘Unwanted and wanted exposure to online pornography in a national sample of youth Internet users’ (2007) 119.2 Pediatrics 247

Wood, N., Political Correspondent, ‘Labour backs Hurd on child pornography.’ *Times* (London, 17 October 1987) accessed 21 February 2015.

Wortley, R. & S. Smallbone, *Internet Child Pornography: Causes, Investigation, and Prevention* (1st, ABC-CLIO 2012) 157

Young, A., ‘Ban child porn, demands 'shocked' Maggie.’ *Daily Mail* (London, 6 September 1977) 12 February 2015

Cases

Adams v DPP [2002] EWHC 438 (Admin)

Anderson [1972] 1 QB 304.

Atkins v Director of Public Prosecutions [2000] 2 Cr. App. R. 248

Attorney General's Reference (No.5 of 1980), Re [1981] 1 W.L.R. 88

Attorney General's Reference (No.89 of 2004)

Collier (Edward John) [2004] EWCA Crim 1411

Daniels [2004] NLSCTD at [33]

DPP v Brooks [1974] AC 862 , 866H

DPP v Whyte [1972] AC 849

John Calder Publications Ltd v Powell [1965] 1 QB 509

MacLennan (Hector Colin) v HM Advocate [2012] HCJAC 94

Martin Secker and Warburg [1954] 2 AER 683.

R v Boyesen (1982) 75 Cr.App.R. 51, 53; [1982] A.C. 768

R v *Collier* [2005] 1 WLR 843

R v Deyemi (Danny) [2007] EWCA Crim 2060

R v Dodd (Jonathan James) [2013] EWCA Crim 660

R v Fellows and Arnold [1997] 1 Cr. App. R. 244

R v G and J [2009] UKHL 13 at para 53

R v Gibson (Richard Norman) [1990] Crim. L.R. 738

R v Graham Westgarth Smith, Mike Jayson [2002] EWCA Crim 683

R v Harrison (Neil John) [2007] EWCA Crim 2976; [2008] 1 Cr. App. R. 29

R v Jonathan Bowden [2000] 1 Cr. App. R. 438

R v Land [1998] 1 Cr App R 301

R v McMurray [1996] 8BNIL n30

R v *McNamara* (1988) 87 Cr App R 246, CA.

R v Miller (David) [2010] EWCA Crim 2883

R v Oliver (Mark David) [2002] EWCA Crim 2766

R v Palmer [2011] EWCA Crim 1286

R v Paul Andrew O'Brien [2006] EWCA Crim 3339

R v Perrin [2002] EWCA Crim. 747

R v Ping Chen Cheung [2009] EWCA Crim 2965

R v Porter [2006] EWCA Crim 560; [2006] 2 Cr. App. R. 25

R v Rowe (Andrew) [2007] EWCA Crim 635

R v S, A[2009] 1 Cr. App. R. 18

R v Sharpe 2001 SCC 2

R v Smith (Graham Westgarth) [2003] 1 Cr. App. R. 13

R v Taylor (Lee Robert) [2011] EWCA Crim 1646

R v Warner [1969] 2 A.C. 256

R v Williams (Orette) [2012] EWCA Crim 2162; [2013] 1 W.L.R. 1200 (CA (Crim Div))

St Albans City and District Council v ICL [1996] EWCA Civ 1296

US v Dost 636 F.Supp.828 (1986)

Your Response Ltd v Datateam Business Media Ltd [2014] EWCA Civ 281

Legislation

Criminal Justice Act 1988

Criminal Justice and Immigration Act 2008

Criminal Justice and Public Order Act 1994

Criminal Justice and Court Services Act 2000

Obscene Publications Acts 1959

Protection of Children Act 1978

Regulation of Investigatory Powers Act 2000

Sexual Offences Act 2003

Additional

1993/94 HC 126 Home Affairs Committee. First report. Computer pornography at 67

1979/80 Cmnd. 7772 Home Office. Report of the Committee on Obscenity and Film Censorship

1987/88 Cm 389 Report of the Commissioner of Police of the Metropolis for the year 1987 at 29

2002/03 HC 639 House of Commons. Home Affairs Committee. Sexual Offences Bill at 79
Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography

Joint Committee on the Draft
Investigatory Powers Bill 'Draft Investigatory Powers Bill'
<http://www.publications.parliament.uk/pa/jt201516/jtselect/jtinvpowers/93/93.pdf> at 30.

Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, *G.A. Res. 54/263, Annex II, 54 U.N. GAOR Supp. (No. 49) at 6, U.N. Doc. A/54/49, Vol. III (2000), entered into force January 18, 2002*

Parliament.uk 'Draft Investigatory Powers Bill call for evidence published' <http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-investigatory-powers-bill/news-parliament-2015/call-for-evidence/> accessed 8th March 2016

Sentencing Council. Sexual Offences Definitive Guideline. (2013) <https://www.sentencingcouncil.org.uk/wp-content/uploads/Final_Sexual_Offences_Definitive_Guideline_content_web1.pdf> accessed 11 June 2015

United Nations Convention on the Rights of the Child, Article 1