Combatting those who intentionally access images depicting child sexual abuse on the Internet: A call for a new offence in England and Wales

Graeme Horsman

Faculty of Computer Science,
Department of Computing, Engineering and Technology,
University of Sunderland,
The David Goldman Informatics Centre,
Sunderland
United Kingdom
SR6 0DD

graeme.horsman@sunderland.ac.uk

Abstract

In England and Wales, there are four main categories of offence surrounding images depicting child sexual abuse, those of making/taking, publishing, distributing and possession. Despite being in force for almost 40 years, it is argued that now, additional regulation is required. In response to technological provision such as private browsing, streaming and encryption which are providing investigative difficulties for digital forensic analysts, this article proposes the need to implement a fifth offence, one of 'intentional accessing' and debates the feasibility and justifications for doing so. This proposal coincides with the recent enactment of the Investigatory Powers Act 2016, which enforces new data retention requirements on Internet Service Providers allowing offender Internet connection records to be stored for up to 12 months and retrospectively investigated.

Keywords: Images depicting child sexual abuse; Internet; data retention; Investigatory Powers Act; crime

1 Introduction

Material that constitutes pornography is subject to debate as attitudes surrounding vulgarity vary along with ever-changing levels of tolerance and acceptability in societies (O'Donnell and Miller, 2007). 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 (MacKinnon, 1985). In seeking sexual gratification, an individual does not have free rein to seek or produce sexualised material of any type, and many jurisdictions have sought to legislate on the type of content that is legally acceptable as a form of imagery. Illegal forms of sexual imagery in England and Wales can generally be categorised into two main types, images depicting child sexual abuse (IDCSA) (it must be noted that this content should not be referred to as pornography (see Horsman (2016) for an elaboration of this discussion)) and extreme pornography; the former remains the focus of this article.

Offences of child sexual abuse often trigger significant public outrage, demonstrated by the recent investigations into Jimmy Saville (BBC News, 2014) and Iain Watkins (BBC News, 2013)). Further, IDCSA which stem from physical acts of child abuse are now arguably considered by today's society as one of the worst form of material that an individual can engage with due to the harm it causes to both the child depicted and to society as a whole (Silbert, 1989). The concerns raised regarding IDCSA in England and Wales have been acknowledged for the past 40 years, leading to the implementation of offences under the Protection of Children Act 1978. Now, the Internet has enabled new forms of child abuse and provides a platform to view child abuse material with relative ease in comparison to before its existence, with IDCSA now widespread online and considered more accessible

than ever before (Akdeniz, 2013; Houtepen, 2014; Seigfried-Spellar, 2014; Seto and Ahmed, 2014).

2 The Internet and IDCSA

Seigfried-Spellar (2014) states that law enforcement are now encountering more cases involving IDCSA because of the Internet, with new sites hosting this content continually being discovered (Powell et al., 2015). Offences surrounding IDCSA are now widespread providing a global regulatory problem (United Nations Office on Drugs and Crime, 2013). The vast majority of prosecutions for IDCSA now involve images that are found on digital storage media in computing equipment (Willmore, 2012) where often they are acquired from online sources. In the United States (U.S.), Wolak et al., (2014) identified during the course of their study 244,920 U.S. computers shared 120,418 unique known IDCSA on the Gnutella peer-to-peer file sharing network. The National Center for Missing & Exploited Children Annual Report (NCMEC, 2014) highlighted that in 2014 it received more than 1.1 million reports to its CyberTipline, of which 98% surrounded IDCSA, with the organisation reviewing 28 million IDCSA to assist law enforcement investigations and victim identification. Within the United Kingdom (UK), since 2009 over 100,000 offences surrounding IDCSA have been recorded (CPS, 2015). Children's charity Barnardo's sexual exploitation services is reported to have 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 (House of Commons, 2013). In the UK alone, it is estimated that approximately fifty thousand individuals are involved in the acquisition and distribution of IDCSA (CEOP, 2013). The volume of IDCSA in circulation has become unmanageable, largely due to the Internet and the regulatory issues it causes. Statistics indicate a relatively large number of individuals are being prosecuted for possessing or creating IDCSA (Lukas, 2013; CPS, 2015). However, in absence of a definitive figure which accurately quantifies both the number of IDCSA in circulation and the actual number of individuals involved with them, it is not possible to establish whether these prosecution numbers represent all or only a small proportion of those interacting with IDCSA.

2.1 Increased Accessibility and the Development of a 'Non-Contact Offender'

As of 2015, the Internet has over 3 billion users world-wide (Statista, 2016) where arguably, with increased accessibility comes a potential increase in the number of offenders interacting with IDCSA online. 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 (Office for National Statistics, 2015). When combined with lowering device costs, the majority of UK households now own a personal computer or mobile smartphone device which offers potential access to sexualised content. The fallout from these technological developments remains that those who want to engage with IDCSA no longer need to be involved physically with acts of child abuse or with those carrying out these acts, effectively creating a non-contact offender who can passively engage with this material online. The Internet offers a seemingly anonymous method of fuelling those who can already be termed as a having a fascination with this material (Diez, 2006).

Non-contact offenders are often dependent on technology in order access and acquire IDCSA and as a result, the Internet has now arguably increased the volume of this type of offender by allowing a wider audience access to it. The Internet has transformed an offence from what would previously have maintained a physical element of child sexual abuse (when IDCSA are being produced), to now one where the only evidence of the offence may exist in cyberspace as individuals seek out and view hosted imagery online (Merdian et al., 2013). Despite providing substantial benefits to society as well as almost single-handedly revolutionising modern day living, the Internet has provided a number of facilities for accessing and acquiring IDCSA (Balfe et al., 2015). Through websites, forums and peer-to-peer sharing, the Internet offers an accessible and affordable source of IDCSA in comparison to more tangible forms such as magazines, photographs or books which prior to

the Internet's popularity formed a predominant source (Balfe et al., 2015). Jenkins (2003) argues that although the acquisition of non-electrical forms of IDCSA is now (and has been for several years) more difficult than digital forms due to the ease that digital data can be created, replicated and transferred across networks. 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 (Phelps and Watt, 2014). Recently, Moore and Rid (2016) identified that the most frequent "use of hidden services through Tor are criminal, including drugs, illicit finance and pornography involving violence, children and animals".

2.2 The Effect of the Internet and Regulatory Attempts

The Internet poses the unique issue of causing the user to become disinhibited and more likely to access material which they would not normally seek out, providing for an "unprecedented degree of inquisitiveness, and the danger is that curiosity hardens into deviance" as inhibitions are lost (O'Donnell and Miller, 2007). Similarly it offers a false sense of protection and a sense of anonymity to the user as they feel that they are not physically identifiable while carrying out their online actions (Horsman, 2016b). Taylor and Quayle (2003) highlight that the Internet provides the environment for which a curiosity surrounding IDCSA can flourish where individuals can seek out material based on their own interests and desires as well as seek communication with self-justifying online communities interested in the illegal material (Krone, 2004).

Calls have been made for Internet service providers (ISPs) 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 (Culture, Media and Sport Committee, 2013). 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 (Culture, Media and Sport Committee, 2013). 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 (Davidson et al., 2012). 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 (Carr and Hilton, 2011). However, such response times are not often witnessed when material is hosted abroad leading to the availability of IDCSA being prolonged, and in some cases reported websites remained in action over 12 months after initial reports were made (Carr and Hilton, 2011). IDCSA may also only be hosted for a limited amount of time, long enough to inform offenders so that they can quickly download the content before the host site is shut down in order to evade regulating authorities (O'Donnell and Miller, 2007).

As well as the ability to report illicit websites, advances in the reliability of website blocking technology (seen since 2006) have made a positive impact on restricting access to IDCSA (McIntyre, 2010). As part of the effort made by the Internet Watch Foundation, the search engines Google and Microsoft's Bing now block results for 100,000 search terms in 158 different languages (BBC News, 2014). Yet changing terminology which is used to reference IDCSA remains a constant battle. 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. Despite moves towards regulating IDCSA, it still remains in circulation online making it difficult to control and penalise offenders. Section 3 provides an analysis of the current legal regulations in force in England and Wales for prosecuting those involved with IDCSA.

3 Existing IDCSA Regulations

Baroness Strange stated, “although we enjoy liberty, we must not allow the edges of decency to be eroded into licentiousness” (House of Lords, 1988). Acts that constitute a crime change over time, geographical location and the development of public morals and values (Silverman and Wilson, 2002), 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 (Jenkins, 2003). Involvement with such material is now widely subject to significant stigmatisation, and, viewed as indefensible, 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 as paedophiles, a term which evokes strong opinions. Paedophiles are defined as those who are sexually attracted to pre-pubescent children and/or material depicting such individuals and are frequently considered “the bogeyman of our age” (Silverman and Wilson, 2002). The word itself strikes fear and outrage into many members of society, sparking emotive reactions and 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 (Silverman and Wilson, 2002). Silverman and Wilson (2002) attribute the rise of public outrage against paedophilia and child offences in the UK to the abduction and murder of Sarah Payne in 2000 (BBC News, 2001) 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, have increased society’s anxiety (Ryder, 2002). Acts of public violence, community unrest and vigilantism against potential suspects are regularly witnessed even in cases following negligent and erroneous media reports (Jewkes and Andrews, 2007).

Although developments surrounding the regulation of illegal imagery and sexualised content in England and Wales have existed since the late 1950's with the Obscene Publication Acts, the main offences surrounding IDCSA can be found in the Protection of Children Act 1978 (PCA78) and Criminal Justice Act 1988 (CJA88). These statutes implement the following four core offences. Under the PCA78 Section 1(1), it is illegal to take (or permit to be taken) or make an IDCSA, to distribute or show an IDCSA and to publish IDCSA. Following the CJA88, having possession of IDCSA was also prohibited under Section 160. Although piecemeal developments through case law and further legislative enactments have occurred throughout the last 28 years, these four fundamental offences have remained persistent. The problem caused by this lack of expansion is that technology has developed to offer numerous services and provision which allow an individual to operate outside the confines of these current restrictions, largely through the Internet.

3.1 A summary of Problem Areas

To provide a brief contextualisation of the problems currently posed under the current regulations in England and Wales, the following point is initially raised.

As it stands in England and Wales, an individual can only be prosecuted for IDCSA related offences if an IDCSA is actually found during an investigation. At which point it can be determined which of the four offences they are subject to. To clarify this point, to be liable for possession of IDCSA, an actual image must be found during an investigation and only then can possession be determined. Similarly to be liable for making/taking, distributing or publishing IDCSA, the IDCSA which was subject to these actions must be identified. Although this may seem sensible it must be considered against the volatility of digital data and the ease of which it can be destroyed. It is argued that the act of intentionally accessing IDCSA in order to view the content is wrong (with arguments for this point supplied in Section 3.1.1); yet English law does not acknowledge this. With this point in mind, it should be highlighted that there is currently no offence in English law of intentionally accessing IDCSA. It is argued that this is an omission in regulations in this area as IDCSA are likely

accessed for sexual gratification, which is arguably achieved when viewed. There should be no requirement for an individual to possess, make, distribute or publish IDCSA before an offence is committed, and intentional accessing should be an act also regulated, and is called for by this article.

Patrolling the act of intentional accessing is also suggested as a response to technological developments, particularly, problem technologies such as in-private browsing sessions, streaming facilities and encryption. These techniques can now allow an individual to access and view IDCSA online without leaving behind sufficient evidence to prosecute for the current offences under the PCA78 and CJA88, and their impact on these offences is discussed in Sections 3.2, 3.3 and 3.4 of this article. Internet services now provide the ability to view IDCSA online but never possess or acquire it on their local device. In essence, a user can now view IDCSA online without leaving tangible evidence of a photograph behind on their local device, which can be found during an investigation to prosecute an individual.

Before examining the impact of developments in technology on IDCSA offences, arguments for the need to regulate those who intentionally access IDCSA are proposed and examined.

3.1.1 Proposed Reasoning for an 'Intentional Accessing' Offence

The implementation of an offence of intentionally accessing IDCSA will impact an already strained workload of existing law enforcement and associated organizations dealing with IDCSA. Therefore, in order to consider the development and implementation of an offence of this type, the following justifications for its potential enactment are debated.

i. As we increase the net, we find more involved in IDCSA

A substantial issue surrounding IDCSA online is the inability to quantify and therefore effectively regulate it. Reports indicate that increasing volumes of IDCSA are being discovered, where the Internet Watch Foundation (2016) reported a 417% increase in reports of IDCSA from 2013 and 68,092 reports confirming IDCSA URLs, a 118% increase from 2014 to 2015. There are two potential reasons for increased rates of discovery. First, there may be greater engagement with IDCSA online and therefore more is being discovered due to more being available. Second, requisite bodies and authorities now have more resources and power to look in more detail at the actions occurring online in relation to IDCSA. Hamilton (2011) states, as we increase the resources dedicated to identifying involvement in IDCSA we discover more cases, and since April 2014, the Internet Watch Foundation has had powers to proactively search for IDCSA online as well as reactively respond to reports (Earl, 2016). Regardless of which of the above points remains the most accurate (and potentially both to varying degrees), 'a widening of the net' in terms of how we regulate online IDCSA with a move to prohibiting access can allow the appropriate authorities to increase their understanding of how IDCSA is created and disseminated online, and, of those who engage with it. From a greater understanding, an inference is made that relevant authorities can develop more effective regulatory strategies with a potential to identify a greater number of child victims and remove them from harm. In turn, prohibiting access may make it possible to interrupt the hosting and dissemination of IDCSA online, which may affect the number of individuals who subsequently possess or disseminate this material further. In addition, as Babchishin et al., (2015, p2) state 'the ease of access to online child pornography may contribute to a new group of offenders who succumb to temptations that they would have otherwise controlled'. Prohibiting access to IDCSA and the deterrent of having an offence of this type may prevent or stem the development of such an offender group and prevent those who harbour a curiosity for IDCSA from becoming involved with it.

ii. An inference that those who seek it, must then want to abuse children

A point frequently mooted by research surrounding child sexual abuse offenders is whether those who interact with IDCSA online will then carry out physical acts of child sexual abuse.

Currently, there is no definitive answer (Aslan et al., 2014; Seto et al., 2010), only inferences that those who seek sexual gratification from viewing IDCSA must also by process of association be interested in acting out such fantasies. Babchishin et al., (2015, p2) highlight that the 'prevalence of sexual interest in children is higher among child pornography offenders than among typical, contact sex offenders against children' drawing reference to their earlier research (Babchishin et al., 2011). In studies by Hanson and Babchishin (2009) and Seto et al., (2010) 12.2% of IDCSA offenders were identified as having a history of contact offending (Merdian et al., 2016). Further, online offenders 'were also found to have greater sexual deviancy' (Babchishin et al., 2015). There are many factors to consider which may indicate a likelihood of re-offending or cross-over offending from imagery to physical abuse, including psychological disorders, life experiences and physiological makeup (Houtepen et al., 2014; Babchishin et al 2014; Eke and Seto, 2012). Research has not yet been able to provide a clear answer, but concerns have been raised. Regulating access to IDCSA may highlight individuals who are on a path to carrying out physical acts of child sexual abuse. In turn, it may only highlight those who have intentions to remain non-contact offenders. Failing to regulate access to IDCSA remains a risk, one which cannot yet be accurately evaluated and in turn has be considered against limited resources and additionally incurred costs by law enforcement to control such actions (the feasibility of which is discussed throughout Section 4).

iii. Should we not acknowledge technological developments and prohibit it?

Many countries have taken steps to patrol IDCSA in terms of possession, distribution, creating and publishing. In doing so, there is an acknowledgement that these acts are wrong and therefore in need of regulation. However, consideration must be given as to the underlying motivations for these regulations. At the heart of many arguments is the harm caused to the child, both physically and mentally. Possession of IDCSA is prohibited as the image itself depicts an illegal act, one which is both harmful to the child depicted but also arguably to society as a whole. Given this, the question must be asked, 'is it too big of a step to take to also regulate access to IDCSA?'. Arguably IDCSA is sought by an individual in order to achieve some level of sexual gratification from it, and this is likely achieved when viewed. Take for instance, the situation of two individuals, one who views IDCSA online (but the image is never stored on their local device – see discussion of private browsing and streaming in Sections 3.2 and 3.3), and the other who views an image previously acquired on their PC (no evidence to raise a making charge). The current legal position in England and Wales defines that the second individual likely commits an offence because they possess the content subject to a legal test of possession (see *R v Porter [2006] [2006] 2 Cr. App. R. 25*), but permits a 'passive look' by the first individual. This appears an arbitrary discrimination between these two acts, which at the core, still involve an individual seeking out IDCSA and driving demand for it.

Intentionally accessing IDCSA within the confines of this article is a proposed offence derived from technological developments fundamentally changing the shape of an offence. Technology now offers access to IDCSA without needing to possess or create the content. The motives of an individual who accesses IDCSA may be similar to that of a potential possessor, to seek sexual stimulation from the imagery. Yet the law in England and Wales currently arguably arbitrarily distinguishes between an individual who captures the content of the image on their local device and another who does not. Despite this, both sets of individuals drive the demand for IDCSA, regardless of whether they seek to possess or just view it, the content in both cases has to be created, present and hosted online to see. Failing to regulate access to IDCSA indirectly suggests that only those who seek to possess (or create, distribute and publish) IDCSA are perceived as encouraging demand for it, which is arguably not accurate.

Canadian legislation has already taken steps to distinguish the act of intentional accessing from that of mere possession. Section 163.1(4.1) of the Criminal Code (R.S.C., 1985, c. C-

46) defines and accessing offence carrying a maximum 10 year sentence, with Section 163.1(4.2) stating that 'a person accesses child pornography who knowingly causes child pornography to be viewed by, or transmitted to, himself or herself''. The regulation of those who access IDCSA was introduced into Canadian law in 2002, following an acknowledgement of the importance of Internet Service Provider information and its use in tracking offenders (Library of Parliament, 2009; Smyth, 2007). Although Canadian statistics dissecting prosecutions by offence type to assess the number of prosecutions obtained under the accessing offence could not be identified (see equivalent CPS (2015, p93) statistics), the accessing offence has remained in force for over 15 years and forms part of a set of regulations put in place to stop any form of interaction with IDCSA and prevent child sexual abuse of this type (Bailey, 2007). Given that steps have already been taken to acknowledge the act of intentionally accessing IDCSA in foreign jurisdictions, it is argued that legislation in England and Wales should do the same.

iv. A chance to respond to technology instead of react

The proposal of an accessing offence provides an opportunity to respond to developments in technology (see Sections 3.2, 3.3 and 3.4 below for detailed examples of technological issues) in order to continue to regulate IDCSA. As societal perceptions of online confidentiality change, privacy enhancing technologies are now more prevalent. When coupled with potential access to IDCSA online, it is not beyond possibility to witness a shift in IDCSA where there is no longer a need to possess IDCSA and offenders can simply just view content online without leaving a trace on their local device. Such a movement would still see a demand for IDCSA, but one where those who are interacting with it are protected. Take for instance the situation where every person from this point on decides to access IDCSA online but never possesses or download a copy of an image to their local machine where they may become liable to prosecution, instead opting to revisit a particular site hosting IDCSA. In such a situation, it is unlikely that law enforcement would deem this a satisfactory state of affairs, given that IDCSA would still be in existence and in demand online. An implemented accessing offence presents an opportunity to proactively tackle the fight against IDCSA instead of waiting and reacting to potential shifts in offender behaviour.

v. The child - is it right not to support the child by preventing access to the material?

The question must be raised as to whether the appropriate authorities and organizations are under a moral obligation to support child victims of produced imagery by prohibiting access to it. It is argued that child victims are vulnerable to suffering psychological harm at the thought of the images documenting their abuse being subject to scrutiny online from others (Michaels, 2008; Martin and Alaggia, 2013). With this acknowledgment, it may seem morally right to take steps to avert access to IDCSA in order to prevent further harm to child victims. An accessing offence may not only play a role of deterrent, but also provide some solace to child victims knowing that the level of regulation around IDCSA prohibits this act, potentially supporting any rehabilitation processes and stopping further harm.

vi. Closing the loop

Regulations surrounding IDCSA in England and Wales currently cover four core actions, but omit to address what this article is proposing as a need for a fifth and final stage to the set of regulations in this area. Prohibition of access is a move which provides an individual seeking IDCSA with no room to manoeuvre. By closing a perceived loophole, there is no method left to an individual in which to interact with IDCSA which would not result in a breach of law. With no scope to interact with IDCSA, there is potential to impact and lessen the production and volume of individuals interacting with it.

To demonstrate the issues posed by technology driving the proposal offered in this article, in-private browsing sessions, streaming facilities and encryption are analysed below and their impact on IDCSA investigations.

3.2 Private-Browsing Sessions

One of the key challenges posed by the Internet and its associated services is that users now have the ability to view IDCSA online whilst leaving minimal trace of this action behind on their device. It is typically these devices which are seized and subsequently examined during an investigation, providing the primary source of evidence from which to base a prosecution attempt. However, techniques such as private browsing are designed to allow users to access content online without the need to download and store it. This is achieved by preventing cached website data and history records from being stored locally, leaving behind minimal traces of a user's online actions.

3.2.1 An Example: How Private Browsing Works in Practice

The Internet browser market is dominated by both Google Chrome and Mozilla's Firefox browsers (W3Schools, 2016), with both offering private browsing functionalities. Private browsing is a fairly recent addition to Internet browser applications, designed for users who 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 remains the same; to prevent information being retained regarding what they have done on-line. 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 (Magnet Forensics, 2016). 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 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 during a forensic investigation indicating this act may not be possible. As a result, we have a scenario where a defendant has accessed IDCSA and likely obtained sexual gratification from it, an act that is not prohibited within the confines of the current offences surrounding IDCSA.

3.2.2 What is the Impact of Private Browsing?

The impact of private browsing is that those who access IDCSA online via private browsing sessions are unlikely to have IDCSA automatically downloaded to their PC and stored in their cache (a process which occurs during normal browsing), which would leave an individual potentially liable for a possession or making offence (subject to evidence of intentional searching) under the range of offences stated in the PCA78 and CJA88. When using private browsing it is likely that no IDCSA which the user has accessed online will be present on the device. Further, there may even be no evidence of Internet history records showing where an individual was looking online despite having accessed this content.

3.3 Media Streaming

Streaming protocols provide the second area of concern. Transmission of media content across the Internet frequently takes place in one of two ways; direct download or via media streaming protocols, where the difference between methods has an impact on the current offence of possession and making/creating IDCSA. A direct download of a media file occurs when a request is sent to a host server, at which point the media in question is sent to the clients' machine and stored on their local storage device, typically some form of hard drive (Sobh, 2008). In comparison, those who stream media via the Internet simply access the content on the host server, where they are able to view or listen to the content without having to wait for the content to download to their machine. In fact, streamed media may never be stored on the clients' computer and it is this fact that currently makes it difficult to

prosecute under the current range of IDCSA offences in England and Wales (Sobh, 2008) (owners of the stream will likely fall within the confines of existing creation, distribution / publishing offences). As with the issues noted above with private browsing, streaming protocols may leave little evidence of the streamed media behind on an individual's device from which a forensic investigation can interpret. This may be particularly troublesome if a user streams media from within a private browsing session.

In the case of streaming a user is actually accessing the media content where in most cases, there is limited evidence of the streamed content in order to infer possession or making of IDCSA. At this point it is necessary to place a caveat on the statement above. Evidence left by streaming is often subject to the streaming protocol in use. Some streaming protocols buffer small quantities of data which are cached to the local machine, as seen with progressive downloading protocols (Begen et al., 2011). Such methods are designed to increase the users experience and performance of the stream, where fragments may be recoverable (for example, small Flash Video (.flv) files in the browser cache) with YouTube having adopted this protocol for its media streaming platform (Begen et al., 2011) (although adaptive streaming protocols are now favoured).

By taking a look at the definitions of the acts involved in the offences surrounding IDCSA it is possible to see how streaming currently fails to fit. Possession denotes a state of having ownership or control, which a person streaming media has neither in regards to the streamed content. Further, as often no content relating to the stream may reside on the local machine, a suspect cannot be said to have made an additional form of IDCSA. Instead, accessing (defined as "the ability, right, or permission to approach, enter, speak with, or use; admittance" (Dictionary.com, 2016)) is the term which describes best the acts of interacting with a media stream. Here a user has the ability to use the stream, yet at no point do they possess the stream other than visually.

3.4 Encryption

Encryption techniques provide the final area of concern highlighted in this article. Encryption involves the obfuscation of information via a computational algorithm, often implemented for purposes of security and protection of information (Microsoft, 2014). 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 (Chatterjee, 2011). Without an encryption key, (essentially a password used to reverse the algorithm returning the data back to its original state) content remains in an unreadable state (Sherwinter, 2006). 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 (encrypts 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. For the digital forensic analyst, an opportunity to acquire or crack the password and decrypt the information may have significant time constraints. Sherwinter (2006) 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. The problem encryption presents in relation to IDCSA remains that those who implement it effectively could prevent an effective investigation into

IDCSA and ultimately preventing law enforcement officials from establishing whether an offence surrounding IDCSA has been committed.

The UK Government introduced The Regulation of Investigatory Powers Act 2000 (RIPA) in order to regulate surveillance techniques and the interception of communications (Akdeniz et al., 2001). However this legislation provides a key tool for preventing offenders from escaping conviction through the use of encryption techniques (Chatterjee, 2011). 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 (Palfreyman, 2009). 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. The problem encryption raises is that subject to password disclosure or breaking the encryption, any evidence stored on an encrypted device cannot be accessed. Encryption is designed to obfuscate data, leaving no indication of what is contained upon the device, making prosecution for possession and making/creating IDCSA practically impossible.

The three technologies discussed above bear one thing in common, they all potentially prevent any IDCSA which an individual has accessed and viewed from being discovered during an investigation. Yet, evidence of what IDCSA an individual has accessed using these provision may still be available from Internet Service Providers. This has led to the proposal for implementing an offence of accessing to combat these issues.

4 A Call for a New Offence: 'Intentional Accessing'

This article calls for the development of a fifth offence, one of 'intentional accessing IDCSA' to add to those existing under the PCA78 and CJA88. An intentional accessing offence is offered as a method for combatting troublesome technologies such as those discussed above. Although there are conflicting reports as to whether viewing encourages contact offender or prevents it (Houtepen, 2014; Long, et al 2012), it is argued that there is an implicit link and preventing access to IDCSA closes what can be perceived as an existing gap in legislation. Further, an intentional accessing offence will allow for the prosecution of those engaging with IDCSA, but that fall outside of current regulations. The problem here is that IDCSA are primarily produced to offer some form of sexual satisfaction to the viewer. This is arguably obtained when the images are accessed and viewed, where there is no longer a requirement to save and store these images for later use (which would subsequently make the offender vulnerable to prosecution for making or possession of IDCSA) if the user chooses not to do so. It can also be seen as a method for stemming the production of new material and a deterrent for those currently involved or considering it.

The act of viewing is defined as 'the action of inspecting or looking at something' (Oxford Dictionaries, 2016). When looking at IDCSA, analogy is drawn to the act of window shopping, where a person can look at content but never engage in a transaction where they are deemed to have taken possession of any items. In addition, a similar shift in culture is witnessed with legitimate pornography, where access to this material via streaming, as opposed to purchasing copies of the material, is now a common process. In context, it remains currently viable for individuals to source IDCSA hosted online, view it, and providing none of that content is downloaded to their local device (cached by their Internet browser) or that it is encrypted and beyond current powers of recovery, operate outside of current offences defined in England and Wales under the CPA78 and CJA88. Although just viewing

IDCSA online may seem like a victimless crime, this is inaccurate, with Michaels (2008) stating that harm is caused to the original child victim depicted in the image because of the knowledge that the image is in circulation with the potential to be viewed, providing a strong motive for implementing an accessing offence. Similarly, by failing to prohibit acts of viewing, there is no deterrent for the act, potentially indirectly driving the production of new material to be hosted online. In addition, it may encourage a shift in culture surrounding IDCSA, where a movement towards the development of 'view only' (content which can be accessed and seen, but not downloaded or acquired) images may be seen as a means to evade current legal regulation. Therefore those who are only accessing IDCSA to view it should be regulated.

Seigfried-Spellar (2014) indicates 'viewers are individuals who did not intentionally or knowingly download any pornographic images of minors; instead, these individuals admitted to searching for and accessing websites in order to view online child pornography'. Although these individuals view the material online, this paper champions the terminology of 'accessing' when defining the offence, for the following reasons. First, access can easily be established objectively via Internet connection records (now facilitated by the Investigatory Powers Act 2016 – see discussion in Section 4.1). Second, in technical terms a user accesses material which ultimately leading to the user viewing the material presented to them on screen. Therefore the term access is preferable to that of viewing to prevent debate arising around whether a suspect has actually visually seen an image on screen.

4.1 How to Implement an Accessing Offence: - The Investigatory Powers Act 2016

In November 2015, the Draft Investigatory Powers Bill (DIPB) was presented to the UK Parliament, designed to replace the Data Retention and Investigatory Powers Act 2014. The UK Parliament stated that the 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 included 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" (Parliament.uk, 2015). The focus of the DIPB was the regulation of communication untaken by criminals and terrorists by allowing their online actions to be examined and the implementation of powers to intercept, collect and analyse communication traffic. The DIPB was subject to public, academic and industry pre-legislative scrutiny (DIPB, 2015, pp.1) and attracted significant media attention, and criticism, having been attributed the name 'Snoopers' Charter' due to its implementation of powers of surveillance (BBC News, 2016). Despite concerns, on November 29th 2016, the Investigatory Powers Act 2016 (IPA16) received royal assent, bringing into force the Investigatory Powers Act 2016.

Of particular interest to the facilitation of the offence of intentional accessing proposed in this paper is the communication data collection and retention requirements. To provide insight on what communication data consists of, the DIPB (pp.12) stated that "communications data is information about communications: the 'who', 'where', 'when', 'how' and 'with whom' of a communication but not what was written or said". One of the focuses of the IPA16 are ICRs. IRCs are records of what user's access online (records of website visits etc.) and are gathered by ISPs (referred to as Telecommunications Operators in the IPA16, see Section 261(10)) and under the IPA16, IRCs must be maintained by ISPs for up to 12 months. The IPA16 places the same obligations on all companies providing services to the UK or in control of communications systems in the UK (DIPB, pp.30). Essentially, this regulation offers law enforcement the ability to evaluate a suspect's conduct online across this period of time and retrospectively analyse their actions.

The powers for data retention in the IPA16 have been met with controversy with suggestions that its measures are invasive, encroaching on an individual's right to privacy and allowing law enforcement to 'snoop' (BBC News, 2015). Yet a public consensus poll undertaken in 2014 by research agency TNS showed 71% of the 1195 people questioned 'think the government should prioritise reducing the threat posed by terrorists and serious criminals even if this erodes peoples' right to privacy' (TNS, 2014). A critical assessment of the IPA16's content and application is beyond the scope of this article, where focus must be drawn to how this legislation can support the implementation of an intentional accessing offence for the regulation of IDCSA.

4.2 How can the IPA16 Support the Regulation of those Intentionally Accessing IDCSA?

The value of using online communication data for detecting and prosecuting those involved in IDCSA cannot be underestimated, where in some circumstances it may be the only way to identify an offender (DIPB, pp.12). The DIPB provided the following insight into the importance of intercepted communication data for the purpose of supporting law enforcement to identify and prosecute those involved in child abuse offences.

> From a sample of 6025 referrals to the Child Exploitation and Online Protection Command (CEOP) of the NCA, 862 (14%) cannot be progressed and would require the provisions in the Investigatory Powers Bill to have any prospect of doing so. That is a minimum of 862 suspected paedophiles, involved in the distribution of indecent imagery of children, who cannot be identified without this legislation. This also means that in some cases law enforcement do not have access to essential data regarding an investigation as it has not been retained – this includes, for example, the identity of an individual suspected of sharing indecent images of children or the people with whom a missing person was last in contact (DIPB, pp.25).

The interception and retention of communication data also played a vital role in the case of Iain Watkins, lead singer of the Lost-prophets band, supporting the identification of those involved (DIPB, pp.14). The 12 month retention of data period defined in the IPA16 is seen as a proportionate response, where countries such as Australia having opted for a retention period of up to two years. Further, Paul Lincoln, director for the Office for Security and Counter Terrorism indicated that nearly half of requests made in child sexual exploitation cases as of 2012 were for data between 10 and 12 months old and was identified as a common starting point for investigations (Joint Committee on the Draft Investigatory Powers Bill, 2015a). The debate on the length of the data retention period has raised concerns particularly in relation to data privacy and the additional costs incurred by ISPs to store this data securely for this period of time. However the need is clear as demonstrated by a survey carried out across 64 law enforcement organisations by Michael Atkinson, Secretary to the National Police Council's Data Communications Group who states the following.

> To give you an example, we covered nearly 10,000 pieces of data and applications. That is what this survey was about. Nine per cent of those applications were for sexual offences. What was interesting was that 37% of that 9% of data that we applied for was more than six months old. We would say, and you can see, that retaining the data for more than six months is very important …
>
> …What is really interesting is a document produced by the Interception of Communications Commissioner's Office on 20 November 2015, only last month, which is a breakdown of communications data and applications. It

> shows over 100,000 communications data applications, 19% of which were in relation to sexual offences. Two things jumped straight out at me. First, this is a 100% increase from the survey that we did in 2012. Secondly, 37% of roughly 19,000 is over 7,000. We would say that, if we retain data for only six months, hundreds if not thousands of suspects for sexual offences would likely evade prosecution (Joint Committee on the Draft Investigatory Powers Bill, 2015c).

Further, Detective Superintendent Matt Long of the Child Exploitation and Online Protection Command at the National Crime Agency stated that of the potential 1,500 referrals received by the National Center for Missing & Exploited Children in the US, the first step in the majority of cases was to analyse communication data (Joint Committee on the Draft Investigatory Powers Bill, 2015c). Further, during Operation Notarise, 745 offenders were arrested nationally, where requests for communication data were made with all, resulting in the safeguarding of 518 children (Joint Committee on the Draft Investigatory Powers Bill, 2015c). It is worth noting that if retention periods dropped to six months, 60% of these offenders would be lost (Joint Committee on the Draft Investigatory Powers Bill, 2015c). Alan Wardle, Head of Policy and Public Affairs, NSPCC, indicated that within the UK, organisations working the with Internet Watch Foundation are very proactive, often removing hosted IDCSA online within two hours. However, the problem remains where foreign territories are hosting IDCSA and live streaming acts of child abuse, reported to be crowdfunded (Joint Committee on the Draft Investigatory Powers Bill, 2015b). The use of retained Internet records is seen as crucial to policing IDCSA online by facilitating the identification of those who interact with this material (Joint Committee on the Draft Investigatory Powers Bill, 2015c). Retention periods of 12 months provide a window of opportunity potentially long enough to process investigations in IDCSA and utilize collected ICRs to facilitate an intentional accessing offence and track down potential offenders (Powell et al, 2015).

4.3 IPA16, ICRs and an ‘Intentional Accessing' Offence

Consider the situation where a suspect has been accessing IDCSA online but effectively deletes any trace of this activity from their local machine, beyond forensic recovery. Where a traditional forensic analysis of a suspect’s device may not reveal the true extent of their actions, ISP maintained ICRs are the only option for establishing this content. By retaining ICRs the necessary data may be available for tying suspect Internet traffic to an offender and what they have accessed online (Home Office, 2014). ICR information can also be used to establish intentional browsing behaviour, showing connections to a website initiated by a user’s device, including visits to IDCSA hosting websites, supporting the identification of those intentionally accessing this content.

Despite private browsing functionalities protecting data from being stored on the defendant’s computer, evidence of their visit to an illegal website (ICRs) is maintained by their ISP (as confirmed by Google (2016) Chromes usage policy), who are now required by the IPA16 to maintain this content. Essentially, private-browsing functionalities implement what can be termed as a ‘locally private’ service, where information regarding their online actions is not private from their service provider (BT, SKY etc.). Similarly, those who stream IDCSA content either via normal browsing protocols or private browsing are not anonymous and can be tracked (subject to the use of anonymisation protocols such as Tor). Essentially an intentional accessing offence would provide a two-pronged attack on IDCSA streams, where streamers of IDCSA fall under existing legislative coverage (creation / distribution) and the individuals streaming the content are prohibited from accessing the content and driving demand for it.

Finally, where encryption is discovered on a device and the content cannot be decrypted, ICRs could potentially indicate the types of content being accessed via the device and potentially stored. In all cases, an intentional accessing offence is a method of prosecuting those who are viewing IDCSA online but taking measures to ensure this content does not become 'findable' during an standard forensic investigation should they be arrested.

Implementing an intentional accessing offence can be seen as a method for expanding current legislative powers in terms of apprehending those engaging with IDCSA. It also provides an offence which 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.

4.3.1 Distinguishing the innocent

The implementation of an accessing offence would increase the range of acts which may incur liability, raising concerns regarding erroneous prosecutions. The act of accessing can in theory be committed in the fraction of a second, where intentional and accidental 'accesses' to IDCSA websites must be considered and distinguished with accuracy. As a result, to achieve this distinction, an accessing offence needs to examine a defendants actions as a whole, considering their course of conduct and therefore consideration of ICRs prior to, and, after an access to a website containing IDCSA need to be examined. This may show an individual who accesses IDCSA as part of a series of browsed websites of this type, or an individual who merely accidentally lands on a website, out of synch with browsing habits and then continues normal browsing. Where one may demonstrate a number of ICRs to numerous IDCSA hosting sites and links within such domains, an innocent browser may only exhibit a single ICR amongst legal websites. By analysing a browsing session as a whole, the volume of accesses to IDCSA hosting websites and the pattern of access can all be taken into account when considering culpability, as well as a counter argument to such acts where this information can be factored into the development of a defence to accessing.

4.4 Counter Arguments Regarding the Implementation of an Intentional Accessing Offence

Justifications for implementing an offence of intentionally accessing IDCSA have been provided in Section 3.1.1; however the practical feasibilities also need to be considered. The imposition of a fifth offence involving IDCSA would add additional burden to an already limited set of resources available to law enforcement. At present, IDCSA provides regulatory issues where the UK government has already acknowledged an inability to process and investigate the number of individuals already believed to be involved (HC Deb 4 July 2013). Therefore, any decision to implement an offence of this type needs to be considered not only against any justifiable need to regulate accessing, but also against whether such an offence could be effectively enforced. In turn, given limitations in available resources, it could be argued that investment should be directed at targeting acts of physical child abuse as opposed to digital offences.

In addition, an intentional accessing offence would be reliant on the imposition of data retention periods under the IPA2016. Now in force, ISP data must be maintained. Acquiring access to this information for the purposes of identifying those accessing known IDCSA websites may prove troublesome as any analysis must be done securely, whilst ensuring the privacy innocent Internet users is not compromised. Processing the data would place an additional encumbrance on ISP resources, which are already likely feeling the strain of the additional requirements of having to retain the significant volumes of user ICRs for the 12 month retention period. As a result, securing access and then compliance to evaluate data in such a way may prove troublesome and in turn, may heighten public contention for the IPA16 and the perceived intrusive surveillance of online behaviour. Enforcement of an accessing offence also relies on the accuracy of ICRs meaning that those who take steps to mask or utilize ananoymisation services such as Tor are unlikely to be traceable. In such cases, an intentional accessing offence may be unenforceable as individuals cannot be

identified. However, this limitation currently applies with the enforcement of existing offences surrounding IDCSA, where reliance is placed on the accuracy of any information packages supplied to law enforcement by ISPs with relation to the tracking of potential distributors of IDCSA online. Accuracy issues would also exist in relation to correctly identifying those who access IDCSA from the masses of normal Internet user data collected by ISPs under the IPA16, where financial and/or criminal liability for misidentification would likely be accrued. This additional responsibility of processing IRCs would unlikely be assumed by ISPs and therefore would likely provide an additional resourcing issue for law enforcement.

A final area of consideration lies with the question, should intentionally accessing IDCSA be an offence? Arguments for this offence have been offered in Section 3.1.1 but counter arguments should be given. In addition, regulatory and resource issues have already been addressed, leaving only contemplation of the fundamental act of accessing. As highlighted by Pritchard et al., (2016) there is a lack of research which can quantify societal perceptions of those who interact with IDCSA and how this act is perceived. Yet, substantial media coverage and reported acts of public outrage suggest that IDCSA is generally considered abhorrent (Horsman, 2016). Pritchard et al's., (2016) study demonstrated that a majority of surveyed participants perceived the act of viewing IDCSA online as a wrongful act, despite being confined to a university student demographic. As of yet, there has been no large scale evaluation of public perceptions of the act of accessing IDCSA online and this remains an area arguably in need of evaluation.

5 Concluding Thoughts

This article calls for the implementation of an offence of intentionally accessing IDCSA as a response to technological developments and the Internet, which currently allow individuals to access and view IDCSA in a way that may prohibit attempts to prosecute individuals engaging in this behaviour under the current range of offences. Functionalities such as private browsing and streaming now mean that there is limited evidential data left behind by those utilising these options to accessing IDCSA online. Where a suspect uses a device to access IDCSA in a way which prevents the image being stored on a suspect's local device, there is no offence of possession or creation. The suspect actions are defined as having 'accessed' IDCSA, which remains an unregulated act. This article offers two contributions, first, arguments for the need to implement an offence of 'intentional accessing', and second, a discussion of the feasibility of implementing an offence of this type and how it can be supported by the recent enactment of the IPA2016.

Such a move can be seen as a 'widening of the net', increasing the scope for prosecuting those involved with IDCSA whilst providing a deterrent for those involved in this form of material in an attempt to stem the flow of existing content and the production of new imagery.

References

Akdeniz, Y.; Taylor, N.; Walker, C., Regulation of Investigatory Powers Act 2000 (1): Bigbrother.gov.uk: State surveillance in the age of information and rights, [2001] Criminal Law Review, (February), pp. 73-90

Akdeniz, Y., 2013. *Internet child pornography and the law: national and international responses*. Ashgate Publishing, Ltd..

Aslan, D., Edelmann, R., Bray, D. and Worrell, M., 2014. Entering the world of sex offenders: an exploration of offending behaviour patterns of those with both internet and contact sex offences against children. Journal of Forensic Practice, 16(2), pp.110-126.

Babchishin, K.M., Hanson, R.K. and Hermann, C.A., 2011. The characteristics of online sex offenders: A meta-analysis. Sexual abuse: a journal of research and treatment, 23(1), pp.92-123.

Babchishin, K.M., Hanson, R.K. and VanZuylen, H., 2015. Online child pornography offenders are different: A meta-analysis of the characteristics of online and offline sex offenders against children. Archives of sexual behavior, 44(1), pp.45-66.

Balfe, M., Gallagher, B., Masson, H., Balfe, S., Brugha, R. and Hackett, S., 2015. Internet child sex offenders' concerns about online security and their use of identity protection technologies: a review. *Child Abuse Review*, *24*(6), pp.427-439.

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

BBC News, 'Cambridge's Internet Watch Foundation leads child abuse clean up' (BBC News Norfolk 2013) <http://www.bbc.co.uk/news/25005541> accessed 15 March 2014

BBC News, 'Jimmy Savile NHS abuse victims aged five to 75' (BBC News 2014a) <http://www.bbc.co.uk/news/uk-28034427> accessed 1 September 2014

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

BBC News (2015) 'Snoopers' charter or protection from terrorists? What the new data monitoring laws should do' Available at: http://www.bbc.co.uk/newsbeat/article/33092771/snoopers-charter-or-protection-from-terrorists-what-the-new-data-monitoring-laws-should-do (Accessed: 8th January, 2016)

BBC News (2016) 'Investigatory Powers Bill: May defends surveillance powers' Available at: http://www.bbc.co.uk/news/uk-politics-35810628 accessed 1 September 2014

Begen, A.C., Akgul, T. and Baugher, M., 2011. Watching video over the web: Part 1: Streaming protocols. *Internet Computing, IEEE*, *15*(2), pp.54-63.

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, great Britain 2011).

CEOP, *Threat Assessment of Child Sexual Exploitation and Abuse*, 2013, 8

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

CPS (2015) 'Violence against Women and Girls Crime Report' Available at: http://www.cps.gov.uk/publications/docs/cps_vawg_report_2015_amended_september_2015_v2.pdf (Accessed: 8th January, 2016)

Davidson, Julia, et al. "Online abuse: literature review and policy context." *European Online Grooming Project. Retrieved March* 9 (2011): 2012.

Dictionary.com (2016) 'access' Available at: http://dictionary.reference.com/browse/accessing?s=t (Accessed: 8th January, 2016)

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

Earl, Alan (2016) 'Partners in prevention - two days at IWF' Available at: https://www.iwf.org.uk/news/partners-prevention-two-days-at-iwf (Accessed 25/02/2017)

Eke, A. W., & Seto, M. C. (2012). Risk assessment of online offenders for law enforcement. In K. Ribisl & E. Quayle (Eds.), Internet child pornography: Understanding and preventing on-line child abuse (pp. 148–168). Devon, UK: Willan

Google 'Browse in private with incognito mode' https://support.google.com/chrome/answer/95464?hl=en-GB

Hamilton, M., 2011. The child pornography crusade and its net-widening effect. Cardozo L. Rev., 33, p.1679

Hanson, R. K. & Babchishin, K. M. (2009, April). How should we advance our knowledge of risk assessment for internet sex offenders? Position Paper prepared for the G8 Global Symposium "Global symposium for examining the relationship between online and offline offences and preventing the sexual exploitation of children", University of North Carolina, Chapel Hill. Retrieved from www.iprc.unc.edu/symposium.shtml

Horsman, G., 2016. Digital forensics: Understanding the development of criminal law in England and Wales on images depicting child sexual abuse. *Computer Law & Security Review*.

Horsman, G., 2016b. The challenges surrounding the regulation of anonymous communication provision in the United Kingdom. *Computers & Security*, *56*, pp.151-162.

House of Commons Deb, 12 June 2013, vol 564, col 399

House of Commons Deb, 4 July 2013, vol 565, col 1142

House of Lords Deb, 17 March 1988 vol 494 cc1251-3

Home Office (2014) 'Counter-Terrorism and Security Bill' Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/388035/CTS_Bill_-_Factsheet_5_-_IP_Resolution_v2.pdf *(Accessed 8th March 2016)*

Culture, Media and Sport Committee, Online Safety (HC 2013, 125-222)

Houtepen, J.A., Sijtsema, J.J. and Bogaerts, S., 2014. From child pornography offending to child sexual abuse: A review of child pornography offender characteristics and risks for cross-over. *Aggression and violent behavior*, *19*(5), pp.466-473.

Internet Watch Foundation (2016) 'Annual Report 2015' Available at: https://www.iwf.org.uk/sites/default/files/inline-files/IWF%202015%20Annual%20Report%20Final%20for%20web_1.pdf

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

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

Joint Committee on the Draft Investigatory Powers Bill (2015a) 'Joint Committee on the Draft Investigatory Powers Bill' Available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/oral/25415.html (Accessed 8th March 2016)

Joint Committee on the Draft Investigatory Powers Bill (2015b) 'Joint Committee on the Draft Investigatory Powers Bill' Available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-

investigatory-powers-bill-committee/draft-investigatory-powers-bill/oral/26563.html (Accessed 8th March 2016)

Joint Committee on the Draft Investigatory Powers Bill (2015c). 'Joint Committee on the Draft Investigatory Powers Bill' Available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/oral/26441.html (Accessed 8th March 2016)

Krone, Tony. *A typology of online child pornography offending*. Australian Institute of Criminology, 2004.

Library of Parliament (2009) 'Bill-C58: Child Protection Act (online Sexual Exploitation)' Available at: http://www.lop.parl.gc.ca/Content/LOP/LegislativeSummaries/40/2/402c58-e.pdf (Accessed 8th May 2017)

Long, M.L., Alison, L.A. and McManus, M.A., 2012. Child pornography and likelihood of contact abuse: A comparison between contact child sexual offenders and noncontact offenders. *Sexual abuse: a journal of research and treatment*, p.1079063212464398.

Lukas, Abby. "Exploring the Extent to Which the Utilization of Technology Has Facilitated the Increased Possession of Online Child Pornography over Time." (2013).

MacKinnon, Catharine A. "Pornography, civil rights, and speech." Harv. CR-CLL Rev. 20 (1985): 1.

Magnet Forensics (2013) 'How does Chrome's 'incognito' mode affect digital forensics?' Available at: https://www.magnetforensics.com/computer-forensics/how-does-chromes-incognito-mode-affect-digital-forensics/ (Accessed 8th March 2016)

Martin, J. and Alaggia, R., 2013. Sexual abuse images in cyberspace: Expanding the ecology of the child. Journal of child sexual abuse, 22(4), pp.398-415.

Mason, S. 'Some international developments in electronic evidence' [2012] Computer and Telecommunications Law Review 23, 30

Merdian, H.L., Curtis, C., Thakker, J., Wilson, N. and Boer, D.P., 2013. The three dimensions of online child pornography offending. *Journal of sexual aggression*, *19*(1), pp.121-132.

Merdian, H.L., Moghaddam, N., Boer, D.P., Wilson, N., Thakker, J., Curtis, C. and Dawson, D., 2016. Fantasy-Driven Versus Contact-Driven Users of Child Sexual Exploitation Material Offender Classification and Implications for Their Risk Assessment. Sexual abuse: a journal of research and treatment, p.1079063216641109.

Michaels R. Criminal law-the insufficiency of possession in prohibition of child pornography statutes: why viewing a crime scene should be criminal. W New Eng Law Rev 2008;30:817–67. p. 818

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

Moore, D. and Rid, T., 2016. Cryptopolitik and the Darknet. *Survival*, *58*(1), pp.7-38.

NCMEC (2014) '2014 Annual Report' vailable at: http://www.missingkids.org/en_US/publications/NCMEC_2014.pdf accessed 28 March 2016

I O'Donnell; C Miller, *Child Pornography; Crime, computers and society* (1st, Willan Publishing, Devon 2007) 259

Office for National Statistics (2015) 'Internet Access - Households and Individuals: 2015' Available at: http://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2015-08-06

Oxford Dictionaries (2016) 'viewing' Available at: http://www.oxforddictionaries.com/definition/english/viewing (Accessed 8th March 2016)

Palfreyman, Brendan M. Lessons from the British and American Approaches to Compelled Decryption; 75 Brook. L. Rev. 363 (2009-2010)

Parliament.uk (2015) 'Draft Investigatory Powers Bill call for evidence published' Available at 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)

Phelps, A. and Watt, A., 2014. I shop online–recreationally! Internet anonymity and Silk Road enabling drug use in Australia. Digital Investigation, 11(4), pp.261-272

Powell, M., Cassematis, P., Benson, M., Smallbone, S. and Wortley, R., 2015. Police Officers' Perceptions of their Reactions to Viewing Internet Child Exploitation Material. *Journal of Police and Criminal Psychology*, *30*(2), pp.103-111.

Prichard, J., Spiranovic, C., Gelb, K., Watters, P.A. and Krone, T., 2016. Tertiary Education Students' Attitudes to the Harmfulness of Viewing and Distributing Child Pornography. Psychiatry, Psychology and Law, 23(2), pp.224-239.

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

Seigfried-Spellar, K.C., 2014. Distinguishing the viewers, downloaders, and exchangers of Internet child pornography by individual differences: Preliminary findings. *Digital Investigation*, *11*(4), pp.252-260.

Seto, M.C., Hanson, R.K. and Babchishin, K.M., 2010. Contact sexual offending by men with online sexual offenses. Sexual Abuse: A Journal of Research and Treatment, p.1079063210369013.

Seto, M.C. and Ahmed, A.G., 2014. Treatment and Management of Child Pornography Use. *Psychiatric Clinics of North America*, *37*(2), pp.207-214.

Sherwinter, Daniel J. Surveillance's Slippery Slope: Using Encryption to Recapture Privacy Rights; 5 J. on Telecomm. & High Tech. L. 514 (2006-2007)

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

J Silverman and D Wilson, *Innocence Betrayed Paedophilia, the Media and Society* (1st, Blackwell Publishing, Cambridge 2002) 193, 2

Smyth, Sara M. "Mind the Gap: A New Model for Internet Child Pornography Regulation in Canada." University of Ottawa Law and Technology Journal 4.1 (2007): 59-108.

Sobh, Tarek (2008) Advances in Computer and Information Sciences and Engineering, SpringerLink: Springer e-Books, Springer Science & Business Media.

Statista (2016) Number of internet users worldwide from 2000 to 2015 (in millions) Available at: http://www.statista.com/statistics/273018/number-of-internet-users-worldwide/ (Accessed 30th March 2016)

Steel, C.M., 2015. Web-based child pornography: The global impact of deterrence efforts and its consumption on mobile platforms. *Child abuse & neglect*, *44*, pp.150-158.

Taylor M & Quayle E. *Child pornography: an Internet crime. (*Hove: Brunner-Routledge, 2003)

TNS (2014) 'Public Opinion Monitor: Britons give safeguarding security a higher priority than protecting privacy' Available at: http://www.tnsglobal.com/uk/press-release/public-opinion-monitor-britons-give-safeguarding-security-higher-priority-protecting-p (Accessed 8th March 2016)

United Nations Office on Drugs and Crime (2013) Comprehensive Study on Cyber Crime pg.26

W3Schools, 'Browser Statistics' (W3Schools 2016) Available at: http://www.w3schools.com/browsers/browsers_stats.asp (Accessed 8th March 2016)

Willmore, Kiel. "Protecting child victims' rights as vigorously as criminal defendants' when prosecuting possession or distribution of child pornography." *Washington Law Review* 87.3 (2012). Pg. 887

Wolak J, Liberatore M, Levine BN. Measuring a year of child pornography trafficking by US computers on a peer-to-peer network. Child abuse & neglect. 2014 Feb 28;38(2):347-56.