Internet Child Sex Offenders' Concerns about Online Security and their Use of Identity Protection Technologies: A Review

Article *in* Child Abuse Review · February 2014

DOI: 10.1002/car.2308

CITATIONS
28

READS
3,338

6 authors, including:

Bernard Gallagher
Independent researcher
17 PUBLICATIONS **202** CITATIONS
SEE PROFILE

Helen Masson
University of Huddersfield
38 PUBLICATIONS **490** CITATIONS
SEE PROFILE

Ruairi Fionnbarra Brugha
Royal College of Surgeons in Ireland
232 PUBLICATIONS **7,857** CITATIONS
SEE PROFILE

Simon Hackett
Durham University
48 PUBLICATIONS **841** CITATIONS
SEE PROFILE

Child Abuse Review(2014)
Published online in Wiley Online Library
(wileyonlinelibrary.com) DOI: 10.1002/car.2308

Internet Child Sex Offenders' Concerns about Online Security and their Use of Identity Protection Technologies: A Review

Myles Balfe*
Department of Sociology, University College Cork, Cork, Ireland

Bernard Gallagher
Helen Masson
Centre for Applied Childhood Studies, University of Huddersfield, UK

Shane Balfe
Internet Security, Deutsche Bank, London, UK

Ruairi Brugha
Department of Epidemiology, Royal College of Surgeons in Ireland, Dublin, Ireland

Simon Hackett
School of Applied Social Sciences, University of Durham, UK

The purpose of this article is to review what is known about the technologies that internet child sex offenders use to abuse or exploit children, offenders' attitudes towards online security and surveillance risk, and their use of identity protection tactics and technologies. The peer-reviewed literature on internet sex offenders published between 2000 and 2011 was surveyed. Internet child sex offenders use a mixture of new and old technologies to abuse children. Offenders' awareness of internet-related risk appears to exist along a continuum. A number of psychological and demographic factors may influence offenders' perceptions of online security risk and their willingness to take security precautions. A surprisingly large number of apprehended offenders in the time period examined by this review did not seem to use any technologies to disguise their identities. A major research programme into internet offenders' use of identity protection technologies, and their use of technologies in general, is needed.

KEY PRACTITIONER MESSAGES:

- Internet child sex offenders use a variety of commonly available technologies, such as social networking sites and peer-to-peer platforms, to abuse children.
- Offenders are a diverse group when it comes to how they perceive risk and act on those perceptions. The risk perceptions and risk management behaviours of individual offenders can be dynamic.
- In the period surveyed by this review (2000–11), some studies found that surprisingly few offenders used technological measures to protect their identities.

KEY WORDS: internet; encryption; child pornography; offender; child sexual abuse

'Internet child sex offenders use a mixture of new and old technologies to abuse children.'

'Surprisingly few offenders used technological measures to protect their identities.'

The internet is a significant resource for child sex offenders. Some offenders use the internet to facilitate non-contact offences, such as

Correspondence to: Myles Balfe, Department of Sociology, University College Cork, Safari Building, O'Donovan's Road, Cork, Ireland. E-mail: mylesbalfe@rcsi.ie

 Accepted: 23 July 2013

downloading child pornography; others for grooming children; and still others use it to network with like-minded individuals (Beech *et al*., 2008; Doring, 2000; Elliott and Beech, 2009; Gallagher, 2007; Schell *et al*., 2007). The internet also provides offenders with a degree of anonymity that they can use – or at least feel that they can use – to avoid detection or thwart investigation. However, although the internet has significant advantages for offenders, it can render some of them more vulnerable to being traced than if they abused offline (Wolak *et al*., 2011).

'There has been a significant amount of research done on the intrapersonal characteristics of internet sex offenders.'

To date, there has been a significant amount of research done on the intrapersonal characteristics of internet sex offenders (the 'sex offender' component of 'internet sex offenders') (Nielssen *et al*., 2011), but researchers, such as Dombrowski and Gischlar (2007) and Prichard *et al*. (2011), have noted that there is little research on the 'internet' component. There is a particular lack of research on the strategies that offenders use to evade detection by law enforcement agencies (Holt *et al*., 2010). To help to begin to address this gap, the authors conducted a review of the peer-reviewed literature on internet child sex offending (published between 2000 and 2011) to examine what is known about these individuals' attitudes towards online security and their use of identity protection techniques and technologies. The review sought to answer the following questions: What internet technologies do child sex offenders use to abuse or exploit children? How conscious are internet sex offenders of the need to protect their identities when they engage in online abuse activities? And what technologies and tactics do offenders use to manage the risk of surveillance?

'An increasing number of organisations involved in responding to the threat of internet child sexual abuse.'

There is an increasing number of organisations involved in responding to the threat of internet child sexual abuse (ICSA). Law enforcement agencies have been at the forefront of this response. These agencies have subsequently been joined by groups concerned with (a) offender treatment, (b) the provision of internet services and (c) agencies involved in the support of children and families. National governments also play a key role in this response, especially in terms of enacting legislation to criminalise particular behaviours or to permit law enforcement monitoring of internet use. There is an increasing pressure upon some of these organisations, in particular those providing internet services, to establish a more effective response to ICSA. All of these organisations need to be aware of the way in which child sex offenders use the internet, if they are to address this problem. This, however, is a challenge, given the minimal amount of research in this area. It is, in light of this fact, essential that full use is made of those data that do exist. It is the aim of this review to highlight the key messages from the research to date in order that all of those concerned with child protection on the internet are more informed as to the manner in which offenders use the internet to bring about child sexual abuse (CSA).

'This review draws together what is known about the technology that offenders use.'

The raison d'être of this review is then, in essence, to facilitate evidence-based practice. This is of most immediate relevance to law enforcement, others involved in the criminal justice system (such as prosecutors and probation staff), along with those charged with treating internet child sex offenders. This review draws together what is known about the technology that offenders use to perpetrate their crimes, the specific purposes to which they put these

DOI: 10.1002/car

technologies and the ways in which they use this technology to manage risk. Possession of this information will enable these agency workers to have an enhanced understanding of both the character and behaviour of offenders. Armed with this knowledge, agency workers should be better equipped to tackle the challenges that offenders present.

Method

The authors searched Pubmed, Web of Science, Psychinfo and Inspec using combinations of the terms: child pornography, indecent image, sex offender (refined with the addition of the keywords: internet, technology, encryption, peer-to-peer (P2P)), grooming (refined with the addition of the keywords: internet, sexual abuse), sexual abuse (refined with the addition of the keywords: internet, technology, encryption, P2P). A total of 689 peer-reviewed articles were identified through this initial keyword database, of which 40 were included in the final review.

'The authors searched Pubmed, Web of Science, Psychinfo and Inspec.'

To be included, articles either had to address the topic of internet sex offenders' technology usage, or the subject of sex offenders and identity and anonymity on the internet. The key reasons for excluding articles were: (a) their subject matter was unrelated to the topics of interest to this review; (b) they focused solely on offenders' non-technological characteristics; (c) they focused on technologies that offenders could potentially use, but did not discuss how sex offenders either used or understood these technologies; and (d) they were review or editorial articles that did not provide additional information beyond what could be obtained from original research articles. The authors included only peer-reviewed articles that were written in English and published between 2000 and 2011. Time and resource constraints meant that the authors were unable to undertake a systematic search of government or police reports on this topic; however, we have included two reports from 2012 that provide additional insights and background information about the problem.

'Two reports from 2012 that provide additional insights and background information.'

What Internet Technologies Do Child Sex Offenders Use to Abuse or Exploit Children?

Offenders use a variety of common technologies to exploit or abuse children, including email, instant messaging, web cams, bulletin boards and 3G phones (Beech *et al*., 2008; Gallagher, 2007; Mitchell *et al*., 2011). A number of offenders continue to use technologies that the general public has largely moved away from, such as newsgroups and chat rooms (Mitchell *et al*., 2010a; O'Halloran and Quayle, 2010). P2P file-sharing seems to be commonly employed by child pornographers, particularly by younger offenders (Kierkergaard, 2011; Latapy *et al*., 2011; Sheehan and Sullivan, 2010; Steel, 2009; Stola *et al*., 2009; Wolak *et al*., 2011). In fact, some researchers have argued that the vast majority of paedophile activity on the internet now occurs on P2P platforms (Kierkergaard, 2011). Recent studies also suggest that offenders are increasingly using social network sites to engage in child abuse activities, especially for grooming-related offences (Mitchell *et al*., 2010a; Quayle and Taylor, 2011). It is unclear why offenders value and use particular technologies; however, theoretical research on how people learn about

DOI: 10.1002/car

technology suggests that familiarity with the specific technology, the technology's ease of use and its perceived usefulness for offenders' goals may be important factors (Venkatesh and Davis, 2000).

'Offenders value the internet more generally for its accessibility, affordability and, perhaps most importantly of all, anonymity.'

Offenders value the internet more generally for its accessibility, affordability and, perhaps most importantly of all, anonymity (Beech *et al*., 2008; Dombrowski *et al*., 2007; Graham, 2000; Mitchell *et al*., 2005a). The internet should, however, be regarded as more of a pseudoanonymising technology rather than a fully anonymising one. Many individuals on the internet can be traced if the tracer has the time and resources to do so (Latapy *et al*., 2011). For example, IP (internet protocol) addresses (identifiers assigned to each device in a computer network) can be automatically logged by programs, websites or peers in P2P file-sharing networks, which can lead the police to an offender's location (Liberatore *et al*., 2010; Wolak *et al*., 2011). The police in some countries frequently use the internet's anonymity to run online 'sting' operations, creating false sexually suggestive personas that will attract offenders (Briggs *et al*., 2011; Mitchell *et al*., 2010b; Urbas, 2010). The truth is that offenders' identities can be discovered on the internet and the web is potentially a risky environment for them (Bourke and Hernandez, 2009; Mitchell *et al*., 2010a, 2011). Eneman (2009), drawing on the work of Michel Foucault, argues that the internet is a *panoptican* environment for child sex offenders, that is an electronic landscape where they are under constant risk of surveillance.

'An electronic landscape where they are under constant risk of surveillance.'

How Concerned Are Internet Sex Offenders About the Risks of Being Detected While Engaging in Online Abuse Activities?

Foucault's work would suggest that given this panoptican context, offenders would become highly concerned about the risk and avoid engaging in behaviours that might facilitate detection by law enforcement. However, the empirical research indicates that offenders' awareness of internet-related risk exists along a continuum. Some offenders, such as individuals who are engaged in contact offences and those who are embedded within internet paedophile networks, are aware of risk and feel that they are – or at least could be – under surveillance from law enforcement agencies (D'Ovidio *et al*., 2009; Eneman, 2009; Holt *et al*., 2010; Ray *et al*., 2010; Sheehan and Sullivan, 2010). Conversely, other researchers have noted that a proportion of internet sex offenders appear to be relatively insensitive to detection risk (Beech *et al*., 2008; Briggs *et al*., 2011; Glasgow, 2010). Indeed, even offenders who are concerned about detection risk can display variable risk awareness, or a variable inclination to act on their risk perceptions (Eneman, 2009).

'Even offenders who are concerned about detection risk can display variable risk awareness.'

Factors That Influence Sex Offenders' Online Perceptions of Risk

A number of studies have identified factors that could underlie and modify offenders' perceptions of internet-related risk.

Demographic Factors

Age might be one risk-related variable, with some studies finding that some young people are 'immature' and 'foolhardy' (Zhang, 2010) in relation to assessing the risks stemming from the creation and distribution of (often

DOI: 10.1002/car

self-generated) indecent images (Kierkergaard, 2011; Quayle and Taylor, 2011). Wolak *et al*. (2008) note that offenders with higher education levels and higher social statuses are sometimes less concerned about detection risk than offenders with less education and who are from lower socio-economic backgrounds, often because they lack criminal experience and suspicion of law enforcement (Wolak *et al*., 2008).

'Offenders with higher education levels and higher social statuses are sometimes less concerned about detection risk.'

Psychological Factors

Offenders who have problems with emotional dysregulation have been found to act spontaneously and often without regard to future consequences when using the internet (Elliott and Beech, 2009). Internet-generated feelings of deindividuation can influence risk-taking perceptions amongst internet sex offenders (Prichard *et al*., 2011). Individuals who access child pornography, or interact with children, in a sexually aroused state may minimise the perceived risk of detection (Prichard *et al*., 2011). Some offenders appear to have an optimistic bias (Eneman, 2009), feeling that while offenders in general are likely to be detected, they in particular are not. A significant proportion of chat room offenders have mental health and substance abuse problems; it seems plausible that individuals with these issues would have problems assessing risk in certain circumstances, or that their risk perceptions could vary according to their mood or substance use (Briggs *et al*., 2011).

'A significant proportion of chat room offenders have mental health and substance abuse problems.'

Social Factors

Being a member of a paedophile forum or network where security concerns are regularly identified and shared can encourage risk awareness amongst some offenders (Eneman, 2009; Holt *et al*., 2010), as can high-profile media coverage of police raids on offender networks (Holt *et al*., 2010).

Technological Knowledge

Offenders with specialised knowledge of internet technologies and computer science may have a greater appreciation of computer-related risk than offenders without this knowledge (Eneman, 2009).

What Technologies and Tactics Do Offenders Use to Manage the Risk of Detection When Engaging in Child Abuse Activities?

Offenders can use a variety of different strategies to manage the risk of detection.

Identity Protection Technologies

A number of offenders use encryption technologies to protect their identities. Armstrong and Forde (2003) note that 'paedophiles are obviously skilled in the use of encryption…as well as the practice of internet anonymity' (p. 212). Kierkergaard (2011) observed that some paedophile forums on the internet are 'heavily encrypted', and Seto *et al*. (2010) found that 80 per cent of a small sample of offenders (n = 20) attempted to hide child pornography content through the use of encryption. Offenders in Eneman's (2010) qualitative study used a variety of technologies, particularly proxy servers, to remain anonymous

'A number of offenders use encryption technologies to protect their identities.'

DOI: 10.1002/car

when downloading child pornography content. Some offenders involved in grooming children use virtual private networks located in other countries to hide their internet traffic (Webster *et al*., 2012).

In contrast to these findings, however, the largest peer-reviewed study of detected child pornography offenders' identity protection technology usage (Wolak *et al*., 2011) found that only three per cent of 604 detected offender cases used encryption (it is unclear whether this figure refers to hard disk or network traffic encryption), and that the proportion of offenders who used encryption appeared to have declined between 2000 and 2006 (the most recent time period looked at by the study). In fact, Wolak *et al*. found that only 19 per cent of their sample used any technical means, including passwords, to hide their child abuse activities. Why more individuals in Wolak *et al*.'s study did not take more technological steps to protect their identities is an interesting question. It may be that they used (ineffective) non-technological means. It may also be that encryption and other security and anonymisation technologies are used by only a proportion of technologically proficient offenders, and that most individuals who access child abuse content do not know how to use it, or think that the 'anonymity' of the internet is sufficient to guarantee their safety. These individuals may think that their risk of being detected is small. Deindividuation caused by internet use may encourage impulsive and disinhibited behaviour in some child pornography offenders (Prichard *et al*., 2011), and the use of identity protection technologies may be less likely when individuals are in this state. Webster *et al*. (2012) were involved in a study of internet groomers where they found that the offenders who were least likely to use identity protection measures were hypersexual men who were almost completely behaviourally unregulated and unconcerned about risk and naive 'intimacy seekers' who felt that they had nothing to hide or be ashamed of about their behaviour. These latter individuals did not employ identity protection technologies because they felt that the use of these technologies would signify that they were doing something 'wrong'. For these individuals, *not* taking steps to protect their identities from discovery appeared to be an identity-preserving measure, one that enabled them to interact with children without experiencing cognitive dissonance. Even offenders who do use identity protection technologies sometimes do so ineffectively, for example, attempting to format a hard disk but leaving substantial child abuse material on it (Wardwell and Smith, 2008).

'The proportion of offenders who used encryption appeared to have declined between 2000 and 2006.'

'The use of identity protection technologies may be less likely when individuals are in this state.'

Disposable Technologies

Some offenders use dedicated computers and smartphones, separate from their regular computers or phones, to access child abuse content (Holt *et al*., 2010). This means that if the offender feels that he has come to the attention of the police he can quickly dispose of the technology without becoming significantly inconvenienced (Holt *et al*., 2010; Webster *et al*., 2012).

'Some offenders use dedicated computers and smartphones, separate from their regular computers or phones.'

Pseudonyms

Individuals involved in child pornography or grooming offences can establish fake identities, for example, employing pseudonymns in chat rooms or on forums/social network sites, or sometimes even pretending to be children

DOI: 10.1002/car

themselves (Graham, 2000; Holt *et al*., 2010; Webster *et al*., 2012). A paedophile forum member in Holt *et al*.'s (2010) study advised other forumites 'don't put any real personal stuff in your online profile' (p. 17). Despite this, offenders sometimes reveal a surprising amount of real-life information in their internet 'handles' such as details about their real-life names, initials, occupations and birthdates (Briggs *et al*., 2011).

Private Communication and Distribution Channels

Offenders can seek to control risk by establishing private communication and distribution channels between themselves. These may be (although they are not limited to) private, restricted chat rooms or private P2P trackers (Kierkergaard, 2011) that are not publicly advertised; information about these channels is passed on only to trusted others. Private communication channels can also be established behind more public (sometimes legal) websites, including social network sites; for example, offenders can join mainstream social network sites and then use the private message functions of those sites to communicate with one another about child abuse-related matters (Mitchell *et al*., 2010a).

'Offenders can seek to control risk by establishing private communication and distribution channels between themselves.'

Avoiding High-Risk Environments

Offenders can manage danger by avoiding what they consider to be high-risk macro- or micro-internet environments. On the macro-scale, offenders often host child abuse material on servers that are located in developing countries in order to take advantage of those countries' lax laws around the possession and distribution of child pornography (Kierkergaard, 2011; Steel, 2009). On the micro-scale, Mitchell *et al*. (2005b) argue that undetected offenders might avoid child abuse websites, or sexual chat rooms, because they know that these sites are the most likely to be patrolled by the police. These offenders may instead focus on accessing images of children, or making contact with children, via non-sexual sites or chat rooms. Offenders can also avoid websites and individuals who they feel could fall under the jurisdiction of their national police force: a UK-based child pornographer in Sheehan and Sullivan's (2010) study noted 'the whole time I had been online I had purposely avoided people from the UK because I was scared of police basically' (p. 153). Offenders can access child abuse content from anonymous venues such as internet cafes; this means that if the IP address of the venue is traced, then the trail will not lead back to them personally. However, it is unclear whether a significant number of offenders engage in these kinds of evasive tactics; 77 per cent of offenders in Wolak *et al*.'s (2011) study accessed child pornography from their home computer, and another three per cent from their work computers.

'Offenders can manage danger by avoiding what they consider to be high-risk macro- or micro-internet environments.'

Offender Groups

Some internet offenders who are actively involved in child abuse activities develop structured networks with like-minded others (Beech *et al*., 2008). These groups use many of the security tactics noted to this point (Elliott and Beech, 2009; Stola *et al*., 2009). Groups are somewhat different from individuals, however, in that they sometimes establish formal, sophisticated security policies, though some groups may be lax about doing

'Groups … sometimes establish formal, sophisticated security policies.'

DOI: 10.1002/car

so (Briggs *et al*., 2011; D'Ovidio *et al*., 2009; Eneman, 2009, 2010; Graham, 2000; Holt *et al*., 2010; Kierkergaard, 2011; Schell *et al*., 2007). Graham (2000) highlighted the security protocols that were used by members of the paedophile website the Wonderland Club, which forced all new members to (a) provide 10 000 unique images of child pornography, (b) be sponsored by existing members of the group and (c) be subject to a formal credibility review by a membership committee. Some groups will also force members to use technologies that the group administrators consider to be secure (Eneman, 2009).

While the strategies employed by groups such as Wonderland (e.g. forced sharing of images) help to maintain network security, they are also potentially risky for the individuals wishing to join those groups. The person who is supplying child abuse material cannot know for sure if the people with whom he is interacting are other offenders or the police. They also cannot know what other offenders will do with any uploaded child abuse material. As a result, some offenders refuse to share their images (Sheehan and Sullivan, 2010). Others do take this risk, either because they perceive that they can gain status within the group or because they feel that the rewards of sharing images (for instance, access to other offenders' images) are greater than the risks of doing so (Gallagher, 2007).

'Some offenders refuse to share their images.'

Offenders often reveal risky personal information once they have joined a group and begun to interact with other group members, often despite the exhortations of group administrators (Eneman, 2009; Gallagher, 2007). When joining a paedophile network, an offender enters a social environment where he can obtain positive feedback, positive reciprocity and emotional congruence, perhaps for the first time in his life (Holt *et al*., 2010). Research on non-internet sex offenders suggests that the longer an offender spends interacting with these kinds of online 'support' networks the greater his likelihood will be of disclosing information about himself (Whitty, 2002). Offenders can also inadvertently reveal clues to their real-life locations simply by the way that they spell certain words when communicating with other group members (Eneman, 2009). Offenders' tendency to 'leak' personal information may be counterbalanced to an extent by the fact that group members often monitor each other's behaviour to ensure that they are being sufficiently secure (Eneman, 2009).

'Offenders can also inadvertently reveal clues to their real-life locations.'

Paedophile Web Forums

Some offenders join paedophile discussion groups or forums where they can discuss their sexual interest in children. These sites usually do not require members to reveal any personal information about themselves. Site administrators often emphasise to members the need to avoid engaging in any activity on the forum that would draw the attention of law enforcement (D'Ovidio *et al*., 2009). When group members post links that could be considered legally risky such as to images or videos of children, administrators often require that multiple proxy links be supplied below each link (Holt *et al*., 2010). Some individuals who discuss possible child abuse activities on these forums frame their activities as 'dreams' that they once had (Holt *et al*., 2010). Therefore, they are not stating that they actually engaged in any illegal activity. As with active offender groups, members of

'Administrators often require that multiple proxy links be supplied below each link.'

DOI: 10.1002/car

paedophile discussion forums often monitor each other's behaviour. When a forum member in Holt *et al*.'s (2010) study informed the group that he was thinking of meeting a boy who he had met over the internet, another forum member noted that the person was getting himself into a very high-risk situation: 'Man, this is dangerous, dangerous, dangerous territory. I hate to burst your bubble, but you should realize that the probability is VERY high that you're talking to the police' (p. 17).

Individuals Who Abuse Children for Commercial Profit

Some researchers have argued that sex offenders will not pay to access child abuse images because of concerns about security risks (i.e. their credit card information will be seized by the police) (D'Ovidio *et al*., 2009; Sheehan and Sullivan, 2010), though it may be that research has not kept up with practice here. Some offenders appear to have stopped paying for child abuse content with traceable currencies, and have instead switched to using anonymous payment systems (Nytimes, 2013). The individuals who actually run commercial child pornography sites – who are often organised criminals (Kierkergaard, 2011) – can use a number of tactics to protect their identities. One is to use a botnet, which is a collection of compromised computers (bots) controlled by a remote command and control infrastructure (Elliott, 2010). Individuals running botnets (called 'botherders') use a technology called fast flux DNS (domain name system) to sell services to individuals who wish to host child abuse content on the compromised computers. The child abuse content will be hosted on a certain subset of the bots. However, the domain name of the child abuse site will point to a different subset of bots in the bot network every minute, making it difficult for law enforcement to trace the exact location of the child abuse content and the individuals running the site (Elliott, 2010). Some offenders advertise children for sale, for sexual abuse, over the internet, but a proportion are subsequently apprehended in undercover police investigations (Mitchell *et al*., 2011). How these offenders decide which 'clients' can be trusted and which cannot is also unknown.

'Some offenders appear to have stopped paying for child abuse content with traceable currencies.'

'How these offenders decide which 'clients' can be trusted and which cannot is also unknown.'

Offenders Who Wish to Contact Children over the Internet

Individuals who seek to make contact with children over the internet, or those seeking to upload recordings of their own abusive actions, would seem to be taking greater risks than individuals who are solely consumers of child abuse material (though we recognise that some non-contact offenders are also involved in undetected contact offences and questionable real-life activities such as travelling to countries known for sex tourism (Bourke and Hernandez, 2009; Niveau, 2010). These individuals can attempt to control risk in several ways. These offenders may be sufficiently manipulative that they are able to move burgeoning online relationships with children offline, aware that online interactions may carry more risks of being detected than 'real-life' interactions (though some offenders only pursue online interactions with children) (Wolak *et al*., 2008). They may seek to move internet communication with the child to a more private communication medium such as email (Webster *et al*., 2012). Offenders often seek to remotely control the child's physical environment, for example, by asking the child if the offender will be overheard by the child's parents, or by blackmailing or threatening the child to

'Offenders often seek to remotely control the child's physical environment.'

DOI: 10.1002/car

keep quiet (Kierkergaard, 2011; Olson *et al*., 2007). Before transmitting identifiable information to a child (such as a picture of themselves), some offenders also take steps to verify the child's identity. However, offenders' risk management strategies can be naive or foolish. For example, chat room offenders seeking to groom children have been reported asking undercover police officers if they are 'under cover girls' (Briggs *et al*., 2011) and social network offenders interested in meeting children for sex have been reported looking at the 'child's' Facebook profile, not considering that the police could also have generated that profile (Mitchell *et al*., 2010a).

Discussion

'Offenders use a mixture of new and old internet technologies to abuse children.'

This is the first study to review what is known about internet sex offenders' use of identity protection techniques and technologies, and the factors that might influence offenders' perceptions of online risk. The review found that offenders use a mixture of new and old (relatively speaking) internet technologies to abuse children. Offenders' perceptions of the risks of using these technologies appear to exist along a continuum. Counter-intuitively, given the seriousness of the consequences for them if they are detected, many offenders do not appear to take steps to protect their identities (Wolak *et al*., 2011), but a proportion do, and these offenders can be quite sophisticated in terms of the countermeasures that they use to combat risk.

There are a number of limitations and gaps in the existing research literature that need addressing. Research on the factors that influence offenders' perceptions of online risk is very limited (especially research on the perceptions of unsecure offenders), despite the work identified in this article. Although no studies have examined the relationships between offenders' perceptions and their security behaviours (Holt *et al*., 2010), there is likely to be a correlation here (Brewer *et al*., 2004). This research would suggest that the offenders who have the greatest risk-related concerns would be the most likely to employ anti-surveillance measures. This makes intuitive sense. However, Brewer *et al*.'s research, and similar work in the health field, is interesting as it suggests that once people take actions to combat risk, their concerns about risk can subsequently decrease. This implies that some offenders who employ security countermeasures may subsequently become less concerned about risk, increasing the likelihood that they would make a security mistake that would render them vulnerable to detection. Furthermore, just because an offender uses a counter-surveillance measure does not mean that measure is sufficient for the threat that the offender is facing (as demonstrated by studies such as Briggs *et al*., 2011). The use of counter-surveillance technologies may therefore give some offenders' the illusion of security rather than true security, and encourage them to engage in excessively risky practices.

'The use of counter-surveillance technologies may therefore give some offenders' the illusion of security.'

The fact that so many offenders do not appear to take technological steps to protect their identities (Wolak *et al*., 2011) or freely or inadvertently provide information about themselves (Briggs *et al*., 2011) is notable, particularly given the catastrophic social and legal consequences for them if they are detected (Gallagher, 2007). A number of offenders likely believe that the 'anonymity' afforded by the internet is sufficient to protect their identities. Others may be careless or impulsive individuals, or believe that the internet is an unreal place where their actions have no real-world consequences, and

DOI: 10.1002/car

therefore there is no need to protect against these consequences (Webster *et al*., 2012). Interpreted via the concepts of the sociologist Erving Goffman, many of these individuals likely see the internet as a 'back-region', a fantasy space where they are free from surveillance. These individuals fundamentally misunderstand that the internet is potentially a giant panoptican, a surveillance machine. However, Wolak *et al*.'s data are seven-years old. Since their data were generated, concerns about government and corporate surveillance of society have gone mainstream in Western nations (Quayle and Taylor, 2011). It is probable that many more people are aware now that they are being tracked every time they go online than would have been the case in 2006. In Goffman's terms, they are aware that the internet is a 'front-region'. Sex offenders are part of the population like everyone else and it is likely that awareness of surveillance risk has increased amongst sex offenders since the mid-2000s. Indeed, recent police reports indicate that offenders' use of encryption and darknet technologies may have increased substantially in the past several years (Child Exploitation and Online Protection Centre, 2012). CEOP estimates that almost half of UK-hidden internet use now involves paedophile activities.

'These individuals fundamentally misunderstand that the internet is potentially a giant panoptican, a surveillance machine.'

'CEOP estimates that almost half of UK-hidden internet use now involves paedophile activities.'

A number of research and practice implications stem from the findings of this review. There is a need: to investigate the factors that offenders use to determine if particular technologies, individuals and websites can be trusted or not; and to use this research to refine online sting operations. We still do not know, for example, how an offender assesses if a particular social network profile is actually that of a child's, and can be safely approached, or a police officer's, and needs to be avoided. To disrupt feelings of perceived anonymity amongst unsecure offenders, it could be useful to have messages 'pop-up' every time that a person enters a child abuse-specific search term (see Steel, 2009, for a list of these terms) into a search engine or P2P platform (Prichard *et al*., 2011). This message could say that, for example, Google or the person's internet service provider has recorded the search together with the person's IP address, or put warnings up saying that particular torrent or websites are being actively monitored by the police and technology companies for child abuse discussions/content.

Conclusion

Internet sex offenders are heterogeneous in terms of how they assess risk and also in how they use technologies such as encryption to protect their identities. For some offenders, identity protection is not a priority; for others, however, detection risk is a significant problem that they are actively attempting to solve. A major research programme is needed to investigate offenders' use of technology, and in particular their use of identity protection technologies. At this point, we have a fairly good understanding of why offenders perpetrate CSA; we now need to know more about how they use technology to facilitate this abuse, avoid detection and thwart investigation.

'We now need to know more about how they use technology to facilitate this abuse, avoid detection and thwart investigation.'

References

Armstrong H, Forde P. 2003. Internet anonymity practices in computer crime. *Information Management and Computer Security* **11**: 209–215.

Beech E, Birgden A, Findlater D. 2008. The Internet and Child Sexual Offending: A Criminological Review. *Aggression and Violent Behaviour* **13**: 216–228.

DOI: 10.1002/car

Bourke M, Hernandez A. 2009. The 'Butner Study' Redux. A Report of the Incidence of Hands-on Child Victimization by Child Pornography Offenders. *Journal of Family Violence* **24**: 183–191.
Brewer N, Weinstein N, Cuite C, Herrington J. 2004. Risk perceptions and their relation to risk behaviour. *Annals of Behavioural Medicine* **27**: 125–130.
Briggs P, Simon W, Simonsen S. 2011. An Exploratory Study of Internet-Initiated Sexual Offenses and the Chat Room Sex Offender: Has the Internet Enabled a New Typology of Sex Offender? *Sexual Abuse* **23**: 72–91.
Child Exploitation and Online Protection Centre. 2012. Threat assessment of child sexual exploitation and abuse. Available: http://ceop.police.uk/Documents/ceopdocs/CEOPThreatA_2012_190612_web.pdf [12 January 2013].
Dombrowski S, Gischlar K. 2007. Safeguarding Young People from Cyber Pornography and Cyber Sexual Predation: A Major Dilemma of the Internet. *Child Abuse Review* **16**: 153–170.
Doring N. 2000. Feminist views of cybersex: victimisation, liberation and empowerment. *Cyberpsychology and Behaviour* **3**: 863–884.
D'Ovidio R, Tyson M, Imanni J, Shumar W. 2009. Adult-Child Sex Advocacy Websites as Social Learning Environments: A Content Analysis. *International Journal of Cyber Criminology* **3**: 1.
Elliott C. 2010. Botnets: To What Extent Are They a Threat to Information Society? *Information Security Technical Report* **15**: 79–103.
Elliott I, Beech A. 2009. Understanding Online Child Pornography Use: Applying Sexual Offense Theory to Internet Offenders. *Aggression and Violent Behaviour* **14**: 180–193.
Eneman M. 2009. Counter-Surveillance Strategies Adopted by Child Pornographers. *International Journal of Technology and Human Interaction* **5**: 1–17.
Eneman M. 2010. Internet Service Provider (ISP) Filtering of Child-Abusive Material: A Critical Reflection of its Effectiveness. *Journal of Sexual Aggression* **16**: 223–235.
Gallagher B. 2007. Internet-Initiated Incitement and Conspiracy to Commit Child Sexual Abuse (CSA): The Typology, Extent and Nature of Known cases. *Journal of Sexual Aggression* **13**: 101–119.
Glasgow D. 2010. The Potential of Digital Evidence to Contribute to Risk Assessment of Internet Offenders. *Journal of Sexual Aggression* **16**: 87–106.
Graham W. 2000. Uncovering and Eliminating Child pornography Rings on the Internet: Issues Regarding and Avenues Facilitating Law Enforcement's Access to 'Wonderland'. *Law Review of Michigan State University* **2**: 457–484.
Holt T, Kristie B, Burker N. 2010. Considering the Pedophile Subculture Online. *Sexual Abuse* **22**: 3–24.
Kierkergaard S. 2011. To Block or Not to Block: European Child Porno Law in Question. *Computer Law and Security Review* **27**: 573–584.
Latapy M, Magnien C, Fournier R. 2011. Quantifying Paedophile Activity in a Large P2P System. *INFOCOM 2011 Proceedings IEEE* 401–405.
Liberatore M, Erdely R, Kerle T, Levine B, Shields C. 2010. Forensic Investigation of Peer-to-Peer File-Sharing Networks. *Digital Investigation* **7**: s95–s103.
Mitchell K, Finkelhor D, Wolak J. 2005a. The Internet and Family and Acquaintance Sexual Abuse. *Child Maltreatment* **10**: 49–60.
Mitchell K, Wolak J, Finkelhor D. 2005b. Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working? *Sexual Abuse* **17**: 241–267.
Mitchell K, Finkelhor D, Jones L, Wolak J. 2010a. Use of Social Networking Sites in Online Sex Crimes Against Minors: an Examination of National Incidence and Means of Utilization. *Journal of Adolescent Health* **47**: 183–190.
Mitchell K, Finkelhor D, Jones L, Wolak J. 2010b. Growth and Change in Undercover Online Child Exploitation Investigations, 2000-2006. *Policing and Society* **20**: 416–431.
Mitchell K, Jones L, Finkelhor D, Wolak J. 2011. Internet-Facilitated Commercial Sexual Exploitation of Children: Findings From a Nationally Representative Sample of Law Enforcement Agencies in the United States. *Sexual Abuse* **23**: 43–71.
Nielssen O, O'Dea J, Sullivan D, Rodriguez M, Bourge D, Large M. 2011. Child Pornography Offenders Detected by Surveillance of the Internet and by Other Methods. *Criminal Behaviour and Mental Health* **21**: 215–224.
Niveau G. 2010. Cyber-Pedocriminality: Characteristics of a Sample of Internet Child Pornography Users. *Child Abuse and Neglect* **24**: 570–575.
Nytimes. 2013. Anonymous payment schemes thriving on web. Available: http://www.nytimes.com/2013/05/30/technology/anonymous-payment-schemes-thriving-on-web.html [7 june 2013].
O'Halloran E, Quayle E. 2010. A Content Analysis of a "Boy Love" Support Forum: Revisiting Durkin and Bryant. *Journal of Sexual Aggression* **16**: 71–85.

DOI: 10.1002/car

Olson L, Daggs J, Ellvold B, Rogers T. 2007. Entrapping the Innocent: Toward a Theory of Child Sexual Predators' Luring Communication. *Communication Theory* **17**: 231–251.
Prichard J, Watters P, Spiranovic C. 2011. Internet Subcultures and Pathways to the Use of Child Pornography. *Computer Law and Security Review* **27**: 585–600.
Quayle E, Taylor M. 2011. Social Networking as a Nexus for Engagement and Exploitation of Young People. *Information Security Technical Report* **16**: 44–50.
Ray J, Kimonis E, Donoghue C. 2010. Legal, Ethical, and Methodological Considerations in the Internet-Based Study of Child Pornography Offenders. *Behavioral Sciences and the Law* **28**: 84–105.
Schell B, Martin M, Hung P, Rueda L. 2007. Cyber Child Pornography: a Review Paper of the Social and Legal Issues and Remedies- and a Proposed Technological Solution. *Aggression and Violent Behaviour* **12**: 45–63.
Seto M, Reeves L, Jung S. 2010. Explanations Given by Child Pornography Offenders for their Crimes. *Journal of Sexual Aggression* **16**: 169–180.
Sheehan V, Sullivan J. 2010. A Qualitative Analysis of Child Sex Offenders Involved in the Manufacture of Indecent Images of Children. *Journal of Sexual Aggression* **16**: 143–167.
Steel C. 2009. Child Pornography in Peer-to-Peer Networks. *Child Abuse and Neglect* **33**: 560–568.
Stola W, Kaspersen H, Kerstensa J, Leukfeldta E, Lodder A. 2009. Governmental Filtering of Websites: the Dutch Case. *Computer Law and Security Review* **25**: 251–262.
Urbas G. 2010. Protecting Children from Online Predators: the Use of Covert Investigation Techniques by Law Enforcement. *Journal of Contemporary Criminal Justice* **26**: 410–425.
Venkatesh V, Davis D. 2000. A theoretical extension of the technology acceptance model: four longitudinal field models. *Management Science* **46**: 186–204.
Wardwell J, Smith S. 2008. Recovering Erased Digital Evidence from CD-RW Discs in a Child Exploitation Investigation. *Digital Investigation* **6**: 6–9.
Webster S, Davidson J, Bifulco A, Gottschalk P, Caretti V, Pham T, Grove-Hills J, Turley C, Tompkins C, Ciullo S, Milazzo V, Schimmerni A, Craparo G. 2012. European grooming project. Available: http://www.europeanonlinegroomingproject.com/wp-content/file-uploads/European-Online-Grooming-Project-Final-Report.pdf [7 june 2013].
Whitty M. 2002. Liar, liar! An examination of how open, supportive and honest people are in chat rooms. *Computers in Human Behaviour* **18**: 343–352.
Wolak J, Finkelhor Mitchell K, Ybarra M. 2008. Online Predators and Their victims: Myths, Realities and Implications for Prevention and Treatment. *American Psychologist* **63**: 111–128.
Wolak J, Finkelhor D, Mitchell M. 2011. Child Pornography Possessors: Trends in Offender and Case Characteristics. *Sexual Abuse* **23**: 22–42.
Zhang X. 2010. Charging Children with Child Pornography: Using the Legal System to Handle the Problem of 'Sexting'. *Computer Law and Security Review* **26**: 251–259.

DOI: 10.1002/car