Cyber crime: A review of the evidence
Research Report 75

Chapter 3: Cyber-enabled crimes - sexual offending against children

Dr. Mike McGuire (University of Surrey) and Samantha Dowling (Home Office Science)

October 2013
Cyber crime: A review of the evidence

Chapter 3: Cyber-enabled crimes – sexual offending against children

Home Office Research Report 75

October 2013

Dr. Mike McGuire (University of Surrey) and Samantha Dowling (Home Office Science)
Acknowledgements

With thanks to: Andy Feist, Angela Scholes, Ian Caplan, Justin Millar, Steve Bond, Jackie Hoare, Jenny Allan, Laura Williams, Amy Everton, Steve Proffitt, John Fowler, David Mair, Clare Sutherland, Magali Barnoux, Mike Warren, Amanda White, Sam Brand, Prof. Majid Yar, Dr. Steve Furnell, Dr. Jo Bryce, Dr Emily Finch and Dr. Tom Holt.

Disclaimer

The views expressed in this report are those of the authors, not necessarily those of the Home Office (nor do they represent Government policy).
## Contents

What are cyber-enabled crimes?  
Key findings: What is known about online grooming?  
  Scale and nature of online grooming  
  Characteristics of Victims  
  Characteristics of Offenders  
Key findings: What is known about the production, possession and distribution of online indecent images of children?  
  Scale and nature of online indecent images of children  
  Characteristics of Victims  
  Characteristics of Offenders  
References
What are cyber-enabled crimes?

Cyber-enabled crimes are traditional crimes, which can be increased in their scale or reach by use of computers, computer networks or other forms of information communications technology (ICT). Unlike cyber-dependent crimes, they can still be committed without the use of ICT. One of the most widely described types of cyber-enabled crime is sexual offending against children.

Key forms of sexual offending against children

Two key forms of sexual offending against children are considered in this chapter.

- **Online grooming** – relates to the use of digital technologies to facilitate either online or offline sexual contact with minors. In an offline setting grooming can take place in a range of locations frequented by children such as parks, schools, parties or shopping centres. In the online context, social networking sites, chat rooms and gaming sites offer the same opportunities for online groomers to befriend children. Some offenders will aim to meet the victim online in order to commit a contact sexual offence, however the internet also enables offenders to limit sexual contact in an online-only environment. In this way they fulfil their sexual motivations without the added risk of meeting a child in person. The Child Exploitation and Online Protection Centre (CEOP) label this form of offending as ‘online child sexual exploitation’ (OCSE), to acknowledge a broader form of offending where many outcomes remain online rather than moving offline (Child Exploitation and Online Protection Centre, 2013a). The offender may adopt the persona of a similarly aged peer when approaching the victim online and may also use blackmail and threats to make the victim comply with their escalating demands (Child Exploitation and Online Protection Centre, 2013a).

- **Proliferation of indecent images of children (IIOC)** – incorporates the use of digital technologies to produce, distribute or possess offensive or indecent images of children. However, the term ‘indecent’ can be hard to define. Legislation in the UK defines Indecent Images of Children (IIOC) as including still and moving images and pseudo-photographs which depict children being sexually abused or exploited. The COPINE scale¹ (Quayle, 2008) systematically attempted to rank the severity of indecent images of children using a ten-point rating system (Taylor et al., 2001; Quayle, 2010) and helped to shape the five-point scale used by the Sentencing Council for England and Wales. The Sentencing Council ‘grades’ indecent images of children in court cases, organised on a scale of increasing seriousness:
  - level 1 nudity or erotic posing with no sexual activity;
  - level 2 non-penetrative sexual activity between children;
  - level 3 non-penetrative sexual activity between adult(s) and child(ren);
  - level 4 penetrative sexual activity between adult(s) and child(ren); and
  - level 5 sadism or bestiality.

¹ Combating Online Paedophile Information Networks in Europe
However, as Quayle (2010, p 347) states “the definitions of such images as ‘abusive’ is a largely subjective one”. For example, identifying whether ‘level 1’ images actually involve sexual activity can be quite challenging. Pseudo images may also be constructed. These are digitally reconstructed photographs where, for example, the head of a child may be photo-shopped onto the body of a woman and the body features manipulated to appear as a child (Quayle and Taylor, 2003; Quayle, 2010). Some images may be wholly constructed and technically involve no ‘victims’.

There is often an overlap between offenders involved in online grooming; those making, distributing or downloading illicit images; and wider, non-contact forms of online abuse, for example, adults engaging young people in cybersex (Bryce, 2010), encouraging young people to watch sexual activity or swapping explicit images of themselves, using webcams (Yar, 2006; Bryce, 2010). Some forms of online sexual abuse may be confined purely to the internet and never progress offline (Child Exploitation and Online Protection Centre, 2013a).

The internet allows for circumvention of the usual protections around children. CEOP identifies four priority themes, which represent key threats for child sexual exploitation and abuse (Child Exploitation and Online Protection Centre, 2013b). Two of these are particularly relevant to the online environment:

- the proliferation of indecent images of children; and
- online child sexual exploitation.

The CEOP report also identified self-generated indecent images (SGII) as a particularly risky online behaviour (Child Exploitation and Online Protection Centre, 2013b). SGII refers to the creation and exchange of sexual images generated by users (although it may include a variety of images or clips posted into online forums). ‘Sexting’ is one of the most common forms of SGII. Whilst it is not always thought of as an offence, images of this sort involving minors could be classified as an indecent image of a child and recorded as a crime.

Other forms of sexual offending may also be facilitated online and whilst serious, are not covered in detail in this chapter. These include the use of online tools to enable human trafficking for sexual purposes; facilitate rape; promote sex tourism or prostitution; the use of webcams or camera phones for voyeuristic ‘peeping tom’ offences; ‘virtual’ sexual offences (for example, involving avatars); and internet-initiated incitement or conspiracy to commit child offences (Durkin, 2007; Gallagher, 2007).

The chapter is divided into two sections. The first focuses on online grooming while the second deals with the creation and generation of indecent images of children.

**Key findings: What is known about online grooming?**

**Scale and nature of online grooming**

**Surveys of young people**

Surveys of children and young people have been undertaken regarding their online experiences, including:

- their experiences of online and offline contact with strangers;
- incidents that caused them ‘concern’; and
- receipt of sexual messages online.
However, it is difficult to draw firm conclusions from these surveys as findings are rarely consistent. This is generally as a result of the different focus of each study, and the varying questions and survey methods used.

Some studies have generated a substantial amount of information on children and young people receiving sexual messages online. However, by no means would all of these constitute an offence and it is unclear whether the messages were received from adults. For instance, Livingstone et al., (2010; 2011) found that 12 per cent of UK children surveyed aged 11 to 16 years reported receiving or seeing sexual messages online in the past 12 months. Overall, three per cent of all UK children (Livingstone et al., 2010; 2011) reported being “bothered” by the sexual message they had received/seen, but again it is unclear what was meant by ‘bothered’ and if this related to online grooming. US surveys report that between 13 per cent (Wolak et al., 2006) and 19 per cent (Finkelhor et al., 2000) of young people aged 10 to 17 years experienced a ‘sexual solicitation’ online. The sensitivity of these topics, however, means that some children will not disclose abuse in a survey setting.

Other studies shed light on the extent to which young people befriend others online (some surveys including teenagers aged 16 years and over). Precise figures vary, but as outlined in Table 3.1, approximately 30 per cent of UK young people aged 9 to 19 years appear to have met or befriended someone they do not know offline, on the internet at some point (Livingstone & Bober, 2005; Eynon, 2009; Livingstone, et al., 2011). A proportion will go on to meet people offline. Livingstone et al., (2010) reported four per cent of UK children in 2010 had met someone offline who they had first met online.

The limited evidence that exists on the outcomes of offline meetings suggests that few actually lead to harm. For example, one per cent of EU children who had met someone online and subsequently met them offline, also expressed concern about what happened when they met. Overall, less than 0.1 per cent reported some form of sexual contact (approximately 28 children) (Livingstone et al., 2011). There is no further explanation about what types of concerns were raised (and the exact figures for the UK are not disaggregated). Bryce (2008) also reports that children surveyed generally viewed offline meetings as positive experiences and an important part of the social networking experience. However, as with all these surveys children may be unlikely to admit inappropriate contact – or be aware that some forms of contact are inappropriate.
### Table 3.1: Numbers and outcomes of young people corresponding and meeting with strangers online and offline

<table>
<thead>
<tr>
<th>Source</th>
<th>Reference/ time period</th>
<th>Sample size</th>
<th>Age group</th>
<th>% of total sample who corresponded with stranger online</th>
<th>% of total sample who made offline contact</th>
<th>% of total sample who were concerned/bothered about the encounter</th>
<th>% with sexual contact following encounter</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK Children Go Online (Livingstone and Bober, 2005)</td>
<td>‘Ever’ done in lifetime. Conducted during January–March 2004.</td>
<td>1,257 (UK children who used the internet at least once a week). Random location sampling.</td>
<td>9–19 years.</td>
<td>30% (377 individuals).</td>
<td>8% (101 individuals).</td>
<td>0.5% (6 individuals) where the new contact turned out to be ‘different’ to what was expected.</td>
<td>N/A</td>
</tr>
<tr>
<td>EU Kids Online, European sample (Livingstone et al., 2011)</td>
<td>‘Ever’ done in lifetime. Conducted during May–June 2010.</td>
<td>25,142 internet using children across 25 EU countries in total. Random stratified sample.</td>
<td>9–16 years.</td>
<td>30% (7,543 individuals).</td>
<td>9% (2,263 individuals).</td>
<td>1% (251 individuals) of all internet-using children reported being bothered by a meeting they had offline.</td>
<td>Less than 0.1% aged 11-16 years (28 individuals).</td>
</tr>
<tr>
<td>EU Kids Online, UK sample (Livingstone et al., 2010)</td>
<td>‘Ever’ done in lifetime. Conducted during May–June 2010.</td>
<td>1,032 internet using UK children. Random stratified sample.</td>
<td>9–16 years.</td>
<td>29% (299 individuals).</td>
<td>4% (41 individuals).</td>
<td>N/A Too small to report reliable findings.</td>
<td>N/A</td>
</tr>
<tr>
<td>Bridging the digital divide (Bryce, 2008)</td>
<td>‘Ever’ done in lifetime.</td>
<td>650 children in North-West of England. Non-random sample.</td>
<td>8–18 years.</td>
<td>62% (403 individuals).</td>
<td>24% (156 individuals).</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Measuring the scale of online grooming faces similar problems to those identified in other chapters of this review. It is very difficult to distinguish between online and offline crimes in police recorded crime measures. The police do not discretely identify cyber-enabled (or cyber-dependent) crimes within police recorded crime. The police generally record offences on the basis of the offence as set out in law and not the medium used to commit it.\(^2\) So an online grooming incident might be recorded as ‘sexual grooming’ within police recorded crime\(^3\) (Home Office, 2010; 2012) and subsequently proceeded and sentenced under legislation such as the Sexual Offences Act 2003.

The numbers of grooming cases recorded by police might suggest that the scale of online and offline forms of grooming is low compared with other forms of serious sexual offending. There were 373 grooming offences (both online and offline) recorded by the police in 2012/13 (Smith et al., 2013), an increase from the 186 offences recorded in 2004/05 (Home Office, 2010), see Table 3.2. In comparison, there were 5,156 offences for rape of a female child under the age of 16 during this same time period. However, online grooming offences may not always be recorded as ‘grooming’, particularly where that grooming results in a more serious offence being committed such as the rape of a child. In such cases the crime recording rules set out that only the most serious offence is recorded by the police under Home Office Counting Rules (HOCR). Furthermore, for grooming to be recorded as an offence under the HOCR, there must also be an offline meeting. In a case where there was only an online meeting, this is likely to be recorded under another sexual offence category.

### Table 3.2: Number of sexual grooming offences recorded by police in England and Wales, 2004/05–2012/13

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sexual Grooming</td>
<td>186</td>
<td>237</td>
<td>322</td>
<td>274</td>
<td>313</td>
<td>393</td>
<td>309</td>
<td>371</td>
<td>373</td>
</tr>
</tbody>
</table>

Source: Home Office (2010), Smith et al. (2013)

Some information on the prevalence of online sexual offending is available from other law enforcement sources though. CEOP’s published data and research on the extent of online grooming are largely based on its operational safeguarding activities and reports received from the public and stakeholders, including the National Society for the Prevention of Cruelty to Children (NSPCC), ChildLine and law enforcement agencies. CEOP generally regard the distinction between online and offline abuse “in many ways artificial to children and young people in 2012” (Child Exploitation and Online Protection Centre, 2012a, p 6) and do not routinely produce data on online/offline grooming. One published report, however, found that of 3,652 reports

---

\(^2\) Police recording of crimes is governed by the National Crime Recording Standard (NCRS) and the Home office Counting Rules (HOCR). These set out the principles under which reports received from victims are recorded. Police recorded crime statistics are based on a notifiable list of offences. The HOCR set out the broad classification groups into which those offences are managed for statistical purposes.

made to CEOP during 2009/10\(^4\) that related to child sex offending, 10 per cent related to online grooming and 16 per cent related to online distribution of images (Child Exploitation and Online Protection Centre, 2010). A further 15 per cent of reports related to possession of indecent images, although it is not clear if all of these were online offences. The remaining reports included contact abuse (both online and offline, 14%), offline grooming (32%) and offline distribution of indecent images (12%) (Child Exploitation and Online Protection Centre, 2010). A 2013 report by CEOP has found that the majority of the 1,145 reports they received from the public in 2012 were confined to the online environment (Child Exploitation and Online Protection Centre, 2013a). In a representative sample of 350 reports from this time period, contact meetings were apparent in just under seven per cent of cases, with the rest of the reports relating to online-only meetings.

As with police recorded crime, sentencing data held by the Ministry of Justice does not identify online from offline offences.

Data provided by the Ministry of Justice show that in 2012, a total of 72 individuals were sentenced for meeting either a female or male child following sexual grooming (Table 3.3).

Table 3.3: Number of individuals proceeded against, found guilty of and sentenced under the Sexual Offences Act, Section 15 (meeting a child following sexual grooming), 2006-2012

<table>
<thead>
<tr>
<th>Legislation and Section</th>
<th>Offence</th>
<th>Outcome</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sexual Offences Act 2003, S.15</td>
<td>Meeting a female child following sexual grooming, etc. – offender aged 18 years and over, and victim aged under 16.</td>
<td>Proceeded against</td>
<td>36</td>
<td>39</td>
<td>36</td>
<td>33</td>
<td>47</td>
<td>49</td>
<td>59</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Found guilty</td>
<td>29</td>
<td>45</td>
<td>38</td>
<td>40</td>
<td>60</td>
<td>51</td>
<td>63</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sentenced</td>
<td>30</td>
<td>46</td>
<td>36</td>
<td>41</td>
<td>62</td>
<td>48</td>
<td>64</td>
</tr>
<tr>
<td>Sexual Offences Act 2003, S.15</td>
<td>Meeting a male child following sexual grooming, etc. – offender aged 18 years and over and victim aged under 16.</td>
<td>Proceeded against</td>
<td>7</td>
<td>2</td>
<td>13</td>
<td>6</td>
<td>8</td>
<td>11</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Found guilty</td>
<td>7</td>
<td>6</td>
<td>10</td>
<td>9</td>
<td>9</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sentenced</td>
<td>7</td>
<td>6</td>
<td>10</td>
<td>9</td>
<td>9</td>
<td>6</td>
<td>8</td>
</tr>
</tbody>
</table>

Source: Ministry of Justice (2013)

Estimating the extent of the problem, however, also depends on young people recognising and reporting their experiences – the scale of under-reporting is not known. Recorded offences are only likely to represent a small proportion of abusive online experiences (Bryce, 2010). In some cases, victims may not realise they have been victimised. For example, Childline (2012) facilitated over 400 counselling sessions for situations where grooming had occurred, 60 per cent of which related to

---

\(^4\) These are reports that related to sexual offending against children only. In total 6,291 reports were made to CEOP during this time period, which also included other types of incidents. Reports were made by the public and other stakeholders (for example, charities).
OCSE. Of these, 82 per cent of the victims did not consider themselves as having been a victim of sexual exploitation. Alternatively, victims may be told not to report by the offender, and/or they may experience self-blame and feelings of shame prevent them from reporting.

Given the similarities between the online grooming process and the general process of forming relationships online, this can make identification of a crime particularly hard for victims, as shown by the following instances.

- The victim may perceive the offender as a friend or partner, rather than as an abuser or offender (Webster et al., 2012) and may believe that they have a romantic relationship with them (Wolak et al., 2004). Offenders may also create fake personas online to portray themselves as similarly aged peers, often of the opposite sex. They use these personas to trick victims into sending self-generated indecent imagery (SGII) (Child Exploitation and Online Protection Centre, 2013b).

- If an offender uses coercive measures to prevent the child from ending the relationship, victims may also be too scared to report the problem, or may simply not know who or where to report.

- Victim gender may also play a role in reporting behaviour – for example, one survey found that boys are less likely than girls to report inappropriate approaches, since they often feel that they can ‘deal’ with it themselves (Webster et al., 2012).

Characteristics of victims

Demographics

In terms of victim characteristics, research generally suggests that girls are most likely to be at risk of online grooming (Bryce, 2010). This is supported by a breakdown of reports of OCSE to CEOP, which show that female victims were apparent in 80 per cent of the 350 reports examined (Child Exploitation and Online Protection Centre, 2013a). US research (Wolak et al., 2006), found that 70 per cent of youths who experienced online approaches were girls.

Some age groups appear more likely than others to receive sexual messages – notably older teenagers – although the available studies often do not specify the precise nature of the communication (whether from strangers, adults, unsolicited). For example, Livingstone et al. (2011) found that 20 per cent of UK 15- to 16-year-olds reported receiving a sexual message online in the past 12 months, compared with 5 per cent of 11- to 12-year-olds. Over 80 per cent of US online grooming victims in Wolak et al.’s (2006) study were also aged over 14 years.

Teenagers may be more vulnerable online than very young children for a number of reasons. For example, they may:

- be more likely to be left unsupervised on the internet by their parents;
- have access to a wider range of online communications tools; and
- also be more curious about relationships and sexuality.

Little is known about the experiences of highly vulnerable young people online, for example, those with special educational needs or disabilities. US research suggests
that young people experiencing depression, loneliness or social isolation, or who have experienced negative life events or maltreatment, may be more at risk, as are those seeking sexual advice or information online (Wolak et al., 2004; Mitchell et al., 2007).

*Risky behaviours*

Both reports in the media and academic literature suggest how disclosure of personal information or images and talking to ‘strangers’ online may leave young people at risk of sexual exploitation (Bryce, 2010). However, large proportions of the population share personal information online and this behaviour underpins online social networking. Given this, other specific behaviours may heighten the risks of online grooming. Research on a sample of US young people who had been groomed for sexual purposes (Wolak et al., 2008) suggests that while posting personal information online does not on its own constitute a key risk factor, communications with an overtly sexual content appear to put users at greatest risk. Some research suggests that the greater the number of risky behaviours undertaken, the greater the risk overall (Mitchell et al., 2007; Ybarra et al., 2007).

Webster et al. (2012) identified 3 broad categories of victims of online grooming through 12 focus groups with young people in the UK, Belgium and Italy.

- *Resilient individuals* are those who act safely and are able to fend off approaches.
- *Risk takers* seek adventure and may be disinhibited. They may engage in multiple risky activities (for example, befriending unknown people online, looking at pornography, being rude or nasty online). They may be open to blackmail by groomers if they can be persuaded to disclose some initial information or images.
- *Vulnerable individuals* seek ‘love’ on the internet and may be particularly susceptible to advances framed in those terms. They may have low self-esteem, which may make interventions difficult since they resist disclosure and believe that they have a ‘true’ relationship, and are not a victim at all.

*Characteristics of offenders*

The research evidence suggests that online groomers are not a homogenous group. There appears to be “no clear demographic profile of offenders involved in the online sexual exploitation of young people other than being male” (Bryce, 2010, p 322). A meta-analysis reviewing characteristics of online offenders suggested that they were more likely to be Caucasian, young, single and unemployed compared with the general population (Babchishin et al., 2011). An in-depth study of 33 male online offenders from the UK, Belgium and Norway, Webster et al. (2012) observed that many had a high IQ, but had not achieved good levels of educational attainment and in this particular study, the majority did not have previous convictions. Howitt and Sheldon (2007) found both Internet and contact offenders were likely to be in a relationship and have children or step children.

Webster et al.’s (2012) qualitative study of 33 online groomers also revealed that these offenders tended to fall into one of three groups (Table 3.4)
Table 3.4: Some characteristics of online groomers

<table>
<thead>
<tr>
<th>Intimacy-seeking offenders</th>
<th>Adaptable-style offenders</th>
<th>Hyper-sexualised offenders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usually did not contact other offenders; viewed their relationship with the victim as “consenting”. Tended not to have indecent imagery of children (IIOC) but did have offline contact. They communicated online with their victim for a long time.</td>
<td>Often had previous convictions and didn’t tend to see their connection with the child as a relationship. Likely to use security measures (for example, hiding online files). Tailored abuse to the child and was involved in offline contact.</td>
<td>Tailored their online identity to the individual child and engaged in sexual contact very quickly. They kept large collections of IIOC and had contact with other sex offenders. Tended to restrict their offending to online contexts and often dehumanised children.</td>
</tr>
</tbody>
</table>

Source: Webster et al. (2012)

Grooming methods

The available research evidence suggests that online grooming techniques appear to have been adapted for the online environment.\(^5\) The accessibility of the internet means that offenders can access and manipulate their victims through a virtual presence and without having to leave their homes. Whittle et al., (2012) suggest that the predominant offline pattern of offenders abusing individuals known to them and in close proximity, may be changing.

O’Connell (2003) and Whittle et al. (2012) outline a number of key stages and processes in online grooming.

- **Identifying/scanning for appropriate victims** – potentially using false information to attract a child into a conversation, or observing open conversations and inviting particular children to a private conversation. US research from mid-2000s found that outright deception (for example, lying about age) was not a common offender tactic (Wolak et al., 2004). However, more recent research from CEOP has found this has become a more common tactic in the UK (Child Exploitation and Online Protection Centre, 2013b).

- **Rapport building and friendship formation** – where the groomer gets to know the child, encouraging them to discuss their life and making an effort to understand their beliefs and circumstances. This serves to build trust and feelings of exclusivity between the offender and the victim.

- **Relationship formation** – where the connection is solidified into something ‘special’ and future plans are discussed, for example, around relationships.

- **Manipulation** – this may involve bribery, flattery, intimidation or more coercive methods, and is aimed to increase dependency on the offender.

\(^5\) Models and pathways for child sexual abuse more generally are outlined in Whittle et al. (2012) and Bryce (2010).
• **Risk assessment** – to establish where the child uses the computer and who else might use it.

• **A sexual stage** – where the offender starts to discuss more overtly explicit themes to normalise sexual language and behaviours. They may also try to get victims to engage in sexual activity, for example, via a webcam or by sending photos.

The timeframe involved in the grooming process may vary between minutes, days, months and years, and differ in style and intensity depending on the offender’s own personality (Whittle *et al.*, 2012). A more recent development in OCSE is perpetrators investing small amounts of time, in large numbers of potential victims, rather than devoting large quantities of time to small numbers of victims (Child Exploitation and Online Protection Centre, 2013a). It is also possible that the relationship may be terminated without meeting the victim. Research has also suggested a distinction between online ‘contact-driven’ offenders, whose goal it is eventually to meet the child (and thereby the grooming process may occur more quickly) and ‘fantasy-driven’ offenders who may be more satisfied with the grooming process itself (and so undertake a longer grooming process, which may not transfer into contact offending). CEOP suggest that grooming in the online environment only may be more common than grooming that is carried out in order to commit contact offence (Child Exploitation and Online Protection Centre, 2013a).

The friendship/relationship stage may be unidentifiable from other online friendships. Wolak *et al.* (2004) suggest that the concept of a ‘stranger’ as a sexual predator may therefore be quite misleading. In a sample of 129 US cases of online sexual contact, they found that the majority of victims were aged 13 to 15 years and were aware of the sexual motivations of the offender. Around three-quarters (74%) of the victims agreed to meet with the offender despite being aware of the sexual aspect and 50 per cent said that they were in love with the offender (Wolak *et al.*, 2004). The study also found there was a lack of obvious coercion in these cases, but it may nevertheless occur to ensure continuing compliance from the victim.

**Offender use of technology**

Some online groomers will exploit ICT in order to identify and contact victims. They use a wide variety of online methods, including: internet relay chat, ICQ (instant messaging); the internet; email; newsgroups; online games; web-cams; social networking; and dating sites for young people (Carr, 2004; Mitchell *et al.*, 2010; Kirwan & Power, 2012; Webster *et al.*, 2012; Child Exploitation and Online Protection Centre, 2013a). Of the 1,145 public referrals to CEOP in 2012, 10 per cent involved OCSE through gaming sites, and 19 per cent involved the use of webcams as part of OCSE (although CEOP state the true figure for webcam use is likely to be substantially higher). Webcams were used by offenders to both capture indecent images of victims, and to show victims indecent images (Child Exploitation and Online Protection Centre, 2013a). Many of the online groomers interviewed by Webster *et al.* (2012) spent a great deal of time online (in some cases more than six hours a day). All offenders in this study said that their use of ICT was determined by how it could best direct them towards children or young adults.

Some offenders may also use sophisticated methods to conceal themselves, although many do not (Carr, 2004). For example:
• purchasing multiple hardware, such as laptops and smartphones, to conceal their location, some specifically used only for offending;
• building elaborate electronic filing systems to store conversations or images, and to hide these activities from others who use the same computer;
• using multiple identities incorporating several internet service providers (ISPs), addresses or proxy servers, to make it look like they are in another country; and
• making changes to their name, age, marital status or online appearance both to entice victims and hide from law enforcement (Webster et al., 2012).

Where new ICT skills were obtained, they appeared to be largely self-taught, for example, through online tutorials (Webster et al., 2012).

Motivations

Motivations for online groomers are clearly sexual; but there may be other motivations too, for example, seeking admiration from victims; or power/control over them; reliving adolescent experiences; being scared of adult relationships; impulse; and curiosity (Wolak et al., 2008). Sexual offending against children may also be driven by other forms of criminality (for example, linked to financial gain).

Wider research in this area has pointed to the disinhibiting effects of internet interaction and the role of cognitive distortions (views that are used to provide rationale or justification to behaviours) in facilitating and driving offending behaviour. These topics are discussed further in other literature, for example, Suler (2004), Howitt and Sheldon (2007), and Whittle et al. (2012).

Key findings: What is known about the production, possession and distribution of online indecent images of children?

The scale and nature of online indecent images of children

There are two main ways of assessing the scale of IIOC:
• the number of IIOC offences recorded by the police, Crown Prosecution Service (CPS) or courts (these may range from possession offences through to making and distributing indecent images); and
• the prevalence of images online.

Police recorded crime, charges and convictions data

Police recorded crime, CPS and Ministry of Justice data record information related to offences involving the production, possession and distribution of indecent images (for example, offences under the Protection of Children Act 1978). It is likely that a large proportion of these offences are now related to electronic formats of images, although this is not known for sure from the data available.

Offences relating to the production of indecent images or pseudo-images of children, along with possession or distribution of these photographs, fall within the Home Office recorded crime category of ‘obscene publications’. However, other offences not related to children or sexual offending are also contained within this same classification and it is not possible to breakdown the category to look at specific
offences relating to indecent images of children. In 2006/07 there were over 2,000 recorded offences involving obscene publications, which increased to over 3,000 by 2012/13 (see Table 3.5).

Table 3.5: Number of recorded crimes in England and Wales for obscene publications, 2006/07–2012/13

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Obscene publications</td>
<td>2,378</td>
<td>2,672</td>
<td>2,775</td>
<td>3,215</td>
<td>3,342</td>
<td>3,321</td>
<td>3,497</td>
</tr>
</tbody>
</table>

Source: Smith et al. 2013

In a representative sample of 610 actionable reports received by CEOP in 2011/12, over one-half related to indecent child images (Child Exploitation and Online Protection Centre, 2012a), although not all of these would necessarily end up recorded as crimes under Home Office Counting Rules.

The CPS records the numbers of charges relating to offences (not numbers of offenders), the data therefore reflect that one offender may receive multiple charges. According to the CPS (see Table 3.6) there were almost 11,000 charges in 2006/07 that involved making an indecent photograph, and numbers increased annually reaching a peak of over 16,000 in 2010/11, before declining to over 15,000 in 2011/12. Similarly numbers of charges for possession of an indecent photograph increased annually from under 3,000 charges in 2006/07 to a peak of over 4,500 in 2010/11, before declining to under 4,000 in 2011/12.

Table 3.6: Offences charged and reaching a first magistrates court hearing 2006/07–2012/13

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Coroners and Justice Act 2009, Ss.62(1) and 66(2)</td>
<td>Possession of a prohibited image of a child.</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>21</td>
<td>179</td>
<td>394</td>
</tr>
<tr>
<td>Criminal Justice Act 1988, S.160(1), (2A) and (3)</td>
<td>Possession of an indecent photograph of a child.</td>
<td>2,768</td>
<td>3,079</td>
<td>4,241</td>
<td>4,117</td>
<td>4,543</td>
<td>3,885</td>
<td>3,849</td>
</tr>
<tr>
<td>Protection of Children Act 1978, Ss.1(1)(a) and 6</td>
<td>Making an indecent photograph of a child.</td>
<td>10,761</td>
<td>11,209</td>
<td>13,824</td>
<td>13,975</td>
<td>16,289</td>
<td>15,226</td>
<td>14,033</td>
</tr>
<tr>
<td>Protection of Children Act 1978, Ss.1(1)(b) and 6</td>
<td>Distributing an indecent photograph of a child.</td>
<td>714</td>
<td>700</td>
<td>949</td>
<td>824</td>
<td>684</td>
<td>743</td>
<td>836</td>
</tr>
<tr>
<td>Protection of Children Act 1978, Ss.1(1)(c) and 6</td>
<td>Showing indecent photographs of children.</td>
<td>501</td>
<td>362</td>
<td>269</td>
<td>137</td>
<td>424</td>
<td>341</td>
<td>317</td>
</tr>
<tr>
<td>Protection of Children Act 1978, Ss.1(1)(d) and 6</td>
<td>Publishing an advertisement likely to suggest that the advertiser distributes or shows indecent photographs of children.</td>
<td>5</td>
<td>19</td>
<td>16</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Source: Crown Prosecution Service

Note 1: Data relates to the number of offences recorded in magistrates’ courts on the Case Management System (CMS).
Note 2: Offences data are not held by defendant or outcome.
Note 3: Offences recorded in the Offences Universe are those which reached a hearing. There is no indication of final outcome or if the charged offence was the substantive charge at finalisation.
Note 4: The CPS does not collect data which constitutes official statistics; these data are provisional and subject to change as more information is recorded by the CPS.
Ministry of Justice data consider the number of offenders proceeded against, found guilty and sentenced under the relevant indecent images legislation (see Table 3.7). These data reveal an increase in number of offenders proceeded against, found guilty and sentenced under Section 1 of the Protection of Children Act 1978 “take, permit to be taken or to make, distribute, or publish indecent photographs or pseudo-photographs of children”. In 2006 over 700 individuals were sentenced under this legislation, rising to over 1,200 individuals in 2012. In 2012, over 200 individuals were sentenced under Section 160 of the Criminal Justice Act 1988 “Possession of an indecent photograph or pseudo-photo”.

Table 3.7: Individuals proceeded against, found guilty and sentenced under legislation relating to sexual images, 2006-2012

<table>
<thead>
<tr>
<th>Legislation and Section</th>
<th>Offence</th>
<th>Proceeded against</th>
<th>Found guilty</th>
<th>Sentenced</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Possession of a prohibited image of a child.</td>
<td>6</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Coroners and Justice Act 2009, Ss.62(1) &amp; 66(2)</td>
<td></td>
<td>15</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Possession of an indecent photograph of a child.</td>
<td>162</td>
<td>162</td>
<td>180</td>
</tr>
<tr>
<td>Criminal Justice Act 1988, S.160</td>
<td></td>
<td>185</td>
<td>191</td>
<td>259</td>
</tr>
<tr>
<td></td>
<td>Take, permit to be taken or to make distribute or publish indecent photographs or pseudo-photographs of children.</td>
<td>937</td>
<td>768</td>
<td>768</td>
</tr>
<tr>
<td>Protection of Children Act 1978, S.1</td>
<td></td>
<td>888</td>
<td>782</td>
<td>753</td>
</tr>
</tbody>
</table>

Source: Ministry of Justice (2013)

The scale of indecent images of children available online

Since 1996 the Internet Watch Foundation (IWF), a UK-based organisation that seeks to minimise worldwide child sexual abuse content on the internet, has collated information on sites displaying IIOC (Internet Watch Foundation, 2013). The IWF provides a hotline/reporting function and works with law enforcement and industry, sharing intelligence and taking action against obscene content and websites online. Its intelligence is generated by reports to its hotline and reports can be made regardless of where websites are located or hosted geographically. In 2012 the IWF reported a decline in the volume of online IIOC reports received (Internet Watch Foundation, 2012). In 2010/11 the IWF processed just over 13,000 URLs reported to contain potentially criminal child sexual abuse content; this declined to just under 10,000 in 2012 (Internet Watch Foundation, 2011; 2012). The IWF confirmed that of the reports received in 2012, 9,550 URLs did actually contain child sexual abuse and the IWF took action against these, for example, by issuing notices to remove obscene content (Internet Watch Foundation, 2012). Of all the child sexual abuse images and videos contained in these URLs (the exact total of images and videos was not reported by the IWF):

- 81 per cent of the child victims appeared under 10 years old;
- 75 per cent of the victims were girls; and
• 53 per cent of all the child sexual abuse URLs depicted sexual activity between adults and children.

However, data from reporting watchdogs rely on internet users finding, identifying and reporting such images. Not all such images will be found unintentionally by everyday internet users. The units of measurement in the IWF reports are also unclear, for example, whether the reports relate to the same images/websites or if they are different or ‘new’ images (the same image could appear on different URLs and domains). It is also unclear what is meant by ‘child sex abuse content’ and whether this relates to images, or other content such as verbal descriptions, which may not be consistent with other definitions of IIOC.

Other research has looked at levels of images on the internet over specific time periods. For example, Renold et al. (2003) found 140,000 IIOC images posted online in various locations over a six-week period in 2002. However, it is not clear if this is an accurate representation of pictures available over different time periods and whether there are seasonal fluctuations in the uploading of IIOC.

Internet service provider statistics can provide some background information on the number of individuals attempting to access IIOC sites. Quayle (2010) reports that one ISP, for example, reported blocking more than 20,000 attempts to access child pornography on the internet in one day. However, it is not clear if this was 20,000 individuals – it is also possible that botnet activity may skew such figures.

**Locations of indecent images of children**

The IWF reported that most images appeared to originate from outside the UK. Of the 9,550 confirmed child sexual abuse URLs in 2012, just 73 were hosted in the UK. Over one-half (54%) were hosted in North America, 37 per cent in Europe and 9 per cent in Asian, South American and African areas (Internet Watch Foundation, 2012). However, hosting may not represent actual distribution but might more accurately represent the distribution of people sending in links. Also where a site is hosted does not indicate where the content was made. Furthermore, hosting data may not be accurate because of site subterfuge and the use of sophisticated sites, hidden from the casual searcher.

The IWF reported that some images are accessed through “disguised websites” where some sites can only be found via a predetermined “digital path” (Internet Watch Foundation, 2011). These sites present the user with different content based on the route they take through the website. When the URL is loaded directly to the browser, it appears as legal adult content. However, if accessed via the digital path, the site displayed child sexual abuse images. This is important for commercial sites to be able to profit from the sale of the content – a child sexual abuse business may be able to acquire legitimate business services, such as banking, if its website appears legitimate. During 2011 this method was identified by the IWF on 579 occasions. Since 2009, 998 unique sources of commercial child sexual abuse websites, with distinctive names and brands were also identified; 440 were active during 2011.

In addition to utilising legitimate website fronts to sell IIOC, CEOP has recognised a trend in the commercial production of IIOC involving the live video streaming of child sexual abuse over webcam. CEOP indicate that this occurs predominantly overseas in vulnerable, deprived countries. A facilitator in the host country agrees and arranges for payments to be made by the offender. These payments will vary in price depending on the requests being made. The relationship of the victim to the
facilitator can vary and may involve family members or associates, however, it has been observed that organised crime groups may also move in at some stage (Child Exploitation and Online Protection Centre, 2013a). The scale of this type of offending is unknown and more work is being conducted by law enforcement to gather further intelligence on these offences.

CEOP estimated that almost half of ‘hidden’ internet use (for example, through The Onion Router (ToR)) involves the proliferation of IIOC. The hidden internet provides users with anonymity and encryption whilst online, and, according to CEOP poses increasing challenges to law enforcement (Child Exploitation and Online Protection Centre, 2012a).

**Characteristics of victims**

**Victims of indecent images**

The IWF analysed the UK-hosted content (73 URLs) in 2012 and found that 79 per cent of child victims were below the age of ten and 51 per cent showed sexual activity between adults and children (Internet Watch Foundation, 2011). A study by the US National Centre for Missing and Exploited Children examining 1,660 images, identified 73 per cent of children as female (Quayle, 2010). There was a fairly even split between pre-pubescent (49%) and pubescent children (45%); 6 per cent of images were described as involving ‘toddlers’. The vast majority of images also related to children of White ethnicity, rather than Asian, Hispanic or Black, and were considered to be from a range of countries. This study was unable to determine how the children came to be part of the photos, what abusive practices they experienced and whether the photos were sold on (Quayle et al., 2008).

‘Sexting’ and self-generated indecent images (SGII)

CEOP suggests that self-generated indecent images represents one of the biggest risks to young people, having seen a recent rise in the numbers of related reports. Of the 2,293 industry reports made to CEOP in 2011/12, 22 per cent related to SGII. Almost one-third were produced by children under 15, but the vast majority were produced by older teenagers. CEOP report that most of these images were believed to be produced without coercion or threat from others and are most commonly uploaded by live one-to-one video chat on websites or via instant messaging applications (Child Exploitation and Online Protection Centre, 2012a).

Similar levels of SGII were found more recently (Child Exploitation and Online Protection Centre, 2013a). Using a sample of 120 still and 113 moving SGII received by CEOP in 2012, it was found that subjects of still SGII were far more likely to be female than male (82% versus 18%), whereas moving SGII is more likely to feature males than females (55% versus 37%). The subjects of both still and moving SGII were White in over 80 per cent of cases. Almost all of the still SGII featured children over 10 (93%) and none could be said to feature children under 10, whereas in moving SGII one-half featured children over 10, and one-third featured children under 10 (Child Exploitation and Online Protection Centre, 2013a). However the difficulty posed to law enforcement by SGII is being able to identify whether the victim in the image has been blackmailed or coerced as this may not be obvious in the picture.

---

6 The ToR helps anonymise online interactions by directing internet traffic through a worldwide network of servers to conceal a user’s original location.

7 Given the nature of the images, it was not possible to identify relevant information in all cases.
although CEOP continue to believe that the majority of images reported to them were freely produced by young adolescents, as part of developmentally appropriate behaviour, rather than as a result of coercive or exploitative behaviour by an adult (Child Exploitation and Online Protection Centre, 2013a).

Surveys of young people suggest that practices such as sexting are now common place. For example, nearly 40 per cent of under 19s in the UK said that they knew friends who exchanged sexual images of themselves or peers by text and 27 per cent said that it happened regularly or all the time (Phippen, 2009). Of the whole sample 30 per cent knew someone who had been adversely affected by this and 56 per cent of respondents were aware of instances where images and videos were distributed further than intended.

Images may be taken and uploaded as part of a joke, an argument, a form of revenge, or as part of consensual sexual activity. It is unclear to what extent SGII may be driven by malevolent intentions of those involved in third-party grooming and abusing children. However, there are concerns about potentially wider exposure of images to individuals unconnected to the victim. The phenomenon of ‘exposure sites’ on Facebook is one such example, where profiles or groups are set up to view images of girls who have ‘sexted’ (Ringrose et al., 2012).

Online child sexual exploitation

In addition to the above consequences, SGII can place the victim at risk of sexual exploitation and can have a serious impact on their mental wellbeing. In the past two years, CEOP has uncovered 184 cases in which victims in the UK were forced to create additional images and videos of themselves by an offender who threatened to share the victim’s SGII with friends, family and their online social network. In some cases, victims were also forced to pose on webcam with degrading messages written on their bodies, or to self harm while the offender watched (Child Exploitation and Online Protection Centre, 2013b) There is a great deal of concern for the welfare of these victims; of the known 184 victims, 6 seriously self harmed or attempted to take their own life and 1 victim committed suicide.

Characteristics of offenders

Several studies have sought to describe the profile of offenders involved in the production and distribution of IIOC images. Henry et al. (2010) examined a group of 633 UK males convicted of IIOC offences (all but 0.2% were convicted of making or taking IIOC images) and found that their average age was around 39 years and that over 80 per cent were either single or divorced (at time of interview). Of the 633 UK males convicted of IIOC offences, 93 per cent were convicted of making images as well as consuming other images, suggesting strong overlaps between viewers and generators.

A study of offenders who committed both IIOC possession offences and contact sex offences against a child was undertaken by CEOP in 2012 (Child Exploitation and Online Protection Centre, 2012b). The sample was made up of 97 case-studies drawn from 34 UK police forces. It found that most offenders were white males, aged between 19 and 45 years. At the time of conviction, most offenders were not in work. Of those who were employed, the single largest group were working in schools or care work, while the remaining offenders were in manual or manufacturing jobs. The majority lived with a spouse or partner and over one-half lived with children.
Offenders tended to have more than one victim (a total of 246 victims were identified from the 97 offenders). Most offenders possessed images up to levels 4 and 5 (the most serious images) and image collection sizes ranged from a handful to 2.5 million.

A recent meta-analysis drew together a large pool of online versus offline offenders (which included IIOC offenders as well as groomers), but struggled to identify clearly groups of online-only offenders from the information reported in previously published research (Babchishin et al., 2011). Comparisons were therefore made between mixed groups of offenders and broadly classed as online or offline. Based on nine comparative studies, the research concluded that online offenders were broadly younger than offline offenders; more likely to be White, and have greater victim empathy and sexual deviancy than offline offenders.

In terms of offenders’ use of technology, the extent to which they conceal their activities or hide their identity has been found to vary. A study of 106 offenders interviewed in New Zealand (Carr, 2004) found that 75 per cent had taken no security measures to protect their images and only a small proportion had applied a password system (8%), encrypted their data (6%) or saved the data to an ambiguously named folder (6%). However, technology and encryption has advanced considerably in recent years, and as mentioned previously, some offenders appear to be using aspects of the hidden internet (such as ToR) to undertake their activities.

The links between online grooming, indecent images of children, and offline sexual offending

Evidence specifically exploring the continuities between the possession of IIOC and other online and offline offending is mixed. Some studies suggest that viewing indecent images of children is often a prelude to committing contact sexual offences against children and is an important risk factor (Calder 2004; Kingston et al., 2008). Around 20 per cent of those involved in online grooming in the US were found to have either taken IIOC or encouraged their victims to send them self-generated IIOC (Wolak et al., 2005). Moreover, one-third of individuals prosecuted for IIOC offences in the UK in 2009 were also found guilty of grooming or sexual offences against children (NSPCC, 2011). Other research refutes such a link or finds much smaller numbers of dual offenders (Smallbone and Wortly, 2000; Seto and Eke, 2005).

CEOP conducted a thematic assessment to understand the link between the possession of IIOC and committing contact sexual abuse of a child (Child Exploitation and Online Protection Centre, 2012b). This analysis found a link between between IIOC possession and the contact sexual abuse of children, however, it was advised that the quantity and level of images an offender holds were “not the most reliable indicators of the risk that these individuals may also be contact sexual offenders” (Child Exploitation and Online Protection Centre, 2012b, p 6).

Beech et al., (2008) identified four groups of images offenders:
- curious and impulsive users;
- users accessing and trading images to fuel sexual interests;
- contact sexual offenders who also use indecent images of children; and
- those who disseminate images for non-sexual reasons, for example, financial gain.

In sum, CEOP states that the links between online and offline sex offences are “heavily contested” (p 5). Possessing IIOC or engaging in online grooming appear to
be risk factors for contact offences, but causation cannot be clearly established. Some offenders may view IIOC before committing a contact offence whilst some IIOC offenders may not commit a contact offence at all (Child Exploitation and Online Protection Centre, 2012b).
References


Child Exploitation and Online Protection Centre (2012b) A Picture of Abuse. London: CEOP.


Coroners and Justice Act 2009.


ISBN: 978-1-78246-245-3