

# Indecent Images & Child Protection

---

The Protection of Children Act of 1978 (as amended) defines what media is considered illegal by the British courts by establishing tests and definitions of indecency and obscenity. There is considerable social stigma attached to this sphere of law, making it an area rarely discussed or debated. Due to the nature of these types of offences, the fact charges often relate to the abuse of minors, and that in many instances computers or communication systems are involved, solicitors and advocates alike can find effective representation difficult.

The Act forbids the creation, showing, distribution, possession for showing or distribution, and advertisement of indecent imagery. As the act was originally developed to consider photographic images, the key concepts and terms used within the legal framework relate to 'making' imagery. As technology has evolved<sup>1</sup>, the act has been interpreted to cover any type of multi-media that might be created or accessed via computer. The later ruling in *R v Bowden* (1999) clarified the position in relation to downloading images or printing them; arguing that such actions are akin to 'making' in a legal sense. Amendments to the act have also rendered illegal 'pseudo-images', artificial or computer generated images, including those where the head of an adult may have been superimposed upon the body of a child. Possession of such material constitutes an offence under the Criminal Justice Act 1988.

In the United Kingdom the concept of indecent, or obscene, media is synonymous with 'Operation Ore' – the British arm of an international Police investigation started in early 2002 to combat child pornography. Despite criticisms<sup>2</sup> of tainted evidence and fundamental failings to corroborate 'facts', it remains an important case study for targeted police activity. To date Operation Ore has resulted in over three and a half thousand arrests, successfully destroyed distribution networks and sent out a powerful message to those that might commit offences of this nature.

To distinguish between child abuse materials, investigators apply images with a relative ranking of severity, based upon the [COPINE Typology](#)<sup>3</sup> designed by the University of Cork. This ten point scheme was distilled by the British courts in the ruling of *R v OLIVER* (2002), creating a sliding scale from, as illustrated in [Figure A](#), which has become the de-facto standard for all related proceedings.

[Lisa Judge](#), specialist criminal barrister from Deans Court Chambers, comments that "sentencing guidelines<sup>4</sup> are based upon categorisation with tariffs reflecting the quantity of images, the severity of such, how long they have been held, whether the materials have been catalogued and organised, how the images were acquired/created, and whether they are a 'trophy of the offender's own sexual abuse of a child'." The threshold for custodial (i.e. prison) sentences is generally accepted to be for imagery at and above level two; although aggravating features such as the duration over which the offences have occurred, size of the cache/collection, and whether there has been incitement to create/make illegal content, are all considered by the courts before applying an appropriate sentence.

---

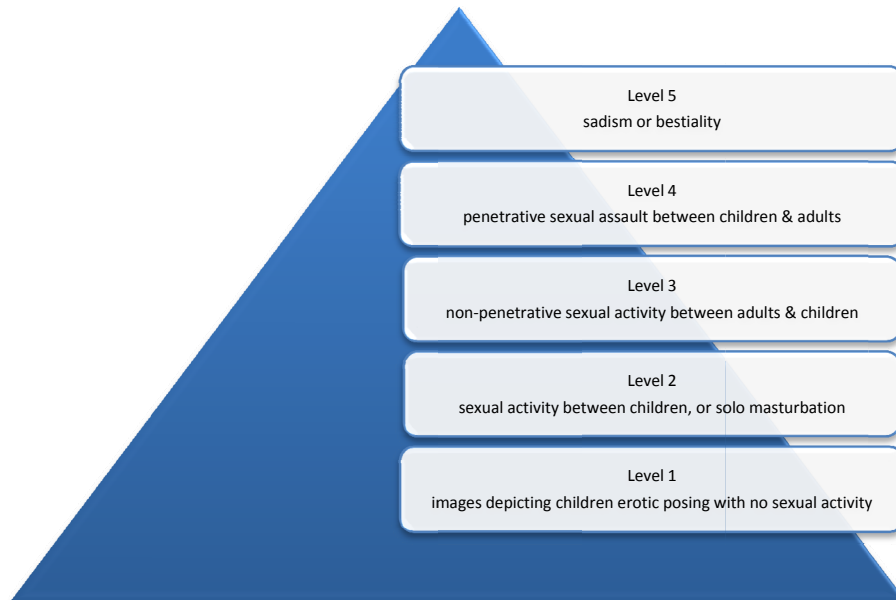
<sup>1</sup> 'Child pornography: an Internet crime', Taylor M & Quayle E 2003

<sup>2</sup> Child porn suspects cleared in evidence 'shambles', Times Online. Ref: [www.timesonline.co.uk/article/0,,2087-1678810,00.html](http://www.timesonline.co.uk/article/0,,2087-1678810,00.html)

<sup>3</sup> 'Combating Paedophile Information Networks in Europe' (COPINE) Project. Reference: [www.copine.ie](http://www.copine.ie)

<sup>4</sup> Sentencing Advisory Panel 2002. The panel's advice to the court of appeal on offences involving child pornography. London: Sentencing Advisory Panel (SAP).

Figure A – R v OLIVER Image Rankings



The nature of this type of offence tends to mean that the imagery has been created using a digital camera, and then transferred to computer for viewing, possible modification and/or distribution. Despite appearing an obvious area for expert assistance, it is common to find that defence teams neglect to instruct a specialist to assist in the development of the defence case.

Computer based evidence is rarely challenged, but this can place the defence at considerable disadvantage and without assessing the accuracy of the findings tendered by the prosecution, such submissions will be accepted by the courts as unassailable fact. Furthermore, if the evidence cannot be examined from a defence perspective, to determine if there is material that is exculpatory (i.e. prove innocence), whether the police investigation has been undertaken in a manner that is consistent with recommended procedures, or to allow any form of independent verification of the prosecution findings.

Forensic analysis of the computer systems and removable media (e.g. floppy disks and CDs) can help answer important questions as to how images came to be created or stored upon the system – and perhaps more importantly what was done with them. Careful forensic examination of the evidence exhibits can provide insights into the following areas:

- Names & addresses of websites visited;
- File-Sharing application used to exchange media;
- Time & dates of last access to a specific file;
- Queries employed by the user on search engines such as Google;
- Attempts made to conceal or remove the media;

Forensic evaluations put the evidence into context and can reveal elements of the case that had previously been unconsidered – which in turn can create significant defence/prosecution case opportunities.

In the majority of cases where contact forensics play a role, such as fingerprints at the scene of crime, a defendant may naturally ‘put the crown to proof’ before deciding on whether to enter a basis of plea with the support of the legal team. In such cases, the defence will naturally instruct an ‘expert witness’ to independently examine the evidence and determine whether there is anything that might materially support or undermine the defence case.

However, in many instances technical evidence is regarded as scientifically perfect and as such a defence is crafted around the findings and attacks against the prosecution case are not made in a head-on fashion. The lack of expert support to assess the technical evidence can place the client at considerable disadvantage. For example, consider the presence of illegal child abuse imagery upon a computer drive. It is important to independently verify the presence and relative severity ranking assigned by the prosecution, but far more important is the detail and story behind the data: when was the file created, was it ever subject to modification, where did it come from, was it sent to a third party, is there peripheral evidence to suggest who was at the keyboard at the time of offence? Finding out the answers to these questions and more helps contextualise the evidence and even in cases of accepted guilt can offer a degree of mitigation that may be taken into account by the courts.

It is important to note that computer forensic consultants that provide expert witness services in respect of indecent images and media must be of the highest calibre and it is necessary for their facilities to be inspected and approved for the undertaking of such work by a Police authority.

## Common Questions

---

*If indecent images have been deleted from the computer can an individual still be charged with possession?*

R v Ross Warwick Porter<sup>5</sup> considered offences that related to the making of indecent photographs of a child under s1(1)(a) Protection of Children Act 1978 and of possessing indecent photographs of children contrary to s160(1) Criminal Justice Act 1988. However, the images in question had been deleted by the defendant before his arrest and were retrieved by the authorities only with the support of specialist forensic technologies and expertise. As a result, the appeal was held and it is now generally accepted that if an individual cannot retrieve or gain access to indecent content, then they cannot be regarded as having custody or control of it.

Note, however, that prosecutors are seeking redress in matters where the ‘Porter ruling’ may be brought into frame, by carefully specifying the dates in the indictment to periods when it can be stated with greater certainty that the imagery was ‘live’ and present upon the computer drive.

---

<sup>5</sup> R v Porter (Ross Warwick) (2006) EWCA Crim 560

*Is it a realistic defence to argue that there was no reason to suspect that the media was potentially illegal and that there is no evidence of actual viewing?*

Whilst the motive behind possession is separate to the question of indecency (R v Graham-Kerr, 1988) the 2004 criminal trial of R v Collier agreed that would be a defensible position in law if it can be shown that an individual had no knowledge or reason to suspect that any multi-media content in their care (or to which they had access) was illegal in nature. This issue is typified in cases involving indecent imagery encountered on the internet, when the web browser ‘caches’ (automatically saves copies of webpages and imagery to the local hard disk without any user intervention). Whilst this action does occur without user intervention, the rulings in *Atkins v DPP* and *Goodland v DPP* (2000) have made it clear that an offence will still have been committed if an ‘internet photo [is] stored automatically on computer’. A defence case built upon reasonable knowledge can be further strengthened by forensic evidence that shows an absence of viewing or access to the indecent media. Operations upon files and folders are recorded in ‘time-stamps’, providing three classes of information; when the file/folder was created, when it was last accessed, and when the file/folder was last modified. Timestamp data is recorded automatically by the operating system and specialist skills and technical understanding is required in order to change these time/date entries – and such tampering can normally be uncovered by astute investigators. In matters of illegal imagery timestamps provide crucial evidence as to actions and put into context when they occurred.

*Can images, which are essentially binary computer code consisting of 1’s and 0’, be considered illegal?*

R v Fellows and R v Arnold (CACD Sep 1996)<sup>6</sup> explored this legal argument and considered whether transformations upon the raw code, such as those that may be necessary to include the data in an e-mail, could affect the legal definition of indecent media. It was held that irrespective of format or transformations, if code can be reconstructed into material with characteristics that would liken it to a photograph or movie, then for the purposes of the law that data would be regarded as media and subject to the same threshold tests of indecency/illegality.

*Provisions contained within Part III of the Regulation of Investigatory Powers Act 2000, due to come into force in October 2007, empower the Police with the right to force the disclosure of encryption keys and passwords.*

*Does making a file available for download indicate exposure or distribution?*

Electronic files can take many forms; from newsgroup postings through to web pages, images or multi-media content such as movies. Such files can be made available for access or duplication using a variety of means (e.g. the inclusion of the file on a website or within a file-sharing application such as ‘Kazaa’). Compounding the legal positioning is the fact that after the initial set-up, the file may be accessed or manipulated without the knowledge or consent of the individual that has made it available. The ruling in R v Skinner (2005) holds that even material automatically copied from one

<sup>6</sup> R v Fellows & Arnold (1997) 1 CAR 224

website to another can be regarded as 'real evidence' and the owner/administrator of the websites in question – as well as those potentially accessing and viewing the content – may be committing criminal offences. Furthermore, the case of *R v Arnold* married the technical and legal arguments, making it clear that the individual responsible for making a file available also distributes it. After this process there may be no more action or intervention by the Defendant, however, the initial positive steps taken are binding and go towards facilitating distribution. Should a 'receiving computer' create a copy of the media, then this only adds gravity to the finding.

### *Is it possible that a website displaying child pornography could 'pop up' on the screen un-requested by the user?*

Many cases involving illegal imagery focus on whether there is evidence of accessing websites that have been confirmed to house child abuse material. A common defence tactic is to suggest that a suspect website was not directly accessed and simply appeared on the screen during the course of browsing the Internet. For instance, the user is surfing website A, when suddenly pages for websites Y and Z appear on the screen – which have not been requested and may contain content quite unlike site A. On pornographic websites of all forms, it is common to have extra browser windows, known as 'pop-ups' to be produced to encourage visitors to view and explore more content than intended. A more modern variant to the 'pop-up' is the '[pop-under](#)', where the browsing window is produced 'minimised' and as such an entire page of content/imagery could load – with fragments potentially 'cached' and saved to the computer drive – without the knowledge or action of the user.

In such cases a comprehensive forensic evaluation of the evidence can reveal if a site was explicitly requested or if a user had been looking for something else but had been directed automatically towards the website in question. Furthermore, it is possible to identify if a given site has been accessed repeatedly (which would challenge any defence that it was an accidental one-off visit) and which areas or categories of the site had been viewed.

### *Understanding the 'Trojan Horse' or 'Third Party' Defence*

There have been a number of high profile cases involving computer abuse/misuse, where the line of defence has been that the computing device had been under the control of an unknown third party. In many cases the assertion is that the computer has been infected by a virus or piece of malicious code that would allow the execution of programs or running of services without either the owner's knowledge or consent. An extension of this theme is to suggest that the computer has been broken into by a Hacker, who used the device as a platform for perpetrating their crime(s). This has become known as the 'Trojan defence' and was applied successfully in the matter of *R v Aaron Caffrey*<sup>7</sup>, who was charged with breaking into computer systems owned by the American port authority in Houston<sup>7</sup>. It has been known for criminals to purposefully infect their computers with viruses and malicious code, laying the foundations for just such a defence should the need ever arise.

<sup>7</sup> Trojan Defence Acquits Teenager, ZDnet Online News. Ref: <http://news.zdnet.co.uk/internet/security/0,39020375,39117209,00.htm>

### *The computer hard disk is second-hand – could the illegal media have originated from actions attributable to the former owner?*

Hard disks, the main storage devices for data and files, are frequently changed between computers – especially when systems are being upgraded or current capacities have been reached and an additional (often cheap second hand) drive is added to increase space for file storage. Few users appreciate the capabilities of data recovery experts and as such tend to simply delete or format their drives before disposal or exchange. Unless a drive has been wiped in accordance with standards<sup>8</sup> such as US DOD 5220.22-M, data can usually be easily retrieved using forensic techniques and sensitive materials may be left residing on a drive long after it has been thought removed by the owner. Whilst the “it was on the drive when I got it” defence is sometimes considered by defendants, it is important to note that skilled forensic examiners will be able to identify times of creation for the images/media and patterns of access which would contradict their account.

### *Obscene media is identified on a shared computer – can the material be attributed to an individual user?*

The classic investigator mantra of ‘who’, ‘what’, ‘where’ and ‘when’ are essential starting points. ‘Who’ considers all the individuals with access and opportunity to the system at the time of the offence – are passwords employed to access the system and/or is the computer in a locked office? ‘What’ explores the nature of the material (e.g. Lolita styled movies) identified, which may itself suggest a particular individual. ‘Where’ asks in what areas of the computer was the data stored – were they public folders accessible to all or restricted portions of the drive available only to authorised users? ‘When’ relies on timestamps and environmental evidence (e.g. personal alibis and/or looking at specific files on the computer that were accessed in and around the time of the offence) to tie many of the complimentary facts together in order to help attribute specific actions with an individual.

---

Rakesh Shah, Partner at specialist criminal defence firm Shah Solicitors, suggests that “given the recent exposure in the press surrounding the disruption of the [‘Son of God’](#) paedophile ring, litigators and layperson alike often believe that this area of crime is on the increase. In fact it is not really getting worse, nor has the internet uniquely facilitated crime of this form, it is that the police are getting better at clamping down on this type of offence and are moving towards a more proactive and intelligence led mode of investigation to help catch offenders at the earliest possible stage. In cases of this nature it is important to consider the evidence in full and consider instructing suitably qualified specialists to aid in reviewing the forensic detail behind the evidence to identify challenges and opportunities.”

*Ross Patel BSc(Hons), MCSE, CISA, CISSP is Director of Hi-Tech Crime at expert witness firm AFENTIS FORENSICS. To find out more about indecent imagery and emerging trends in technology investigation, contact Joanne Davies on 0800 180 4545 or email [jdavies@afentis.com](mailto:jdavies@afentis.com)*

---

<sup>8</sup> United States Department of Defense specification for secure removal of data stored on magnetic media (e.g. computer drives). DOD 5220.22-M. Reference: [http://en.wikipedia.org/wiki/US\\_DOD\\_5220.M](http://en.wikipedia.org/wiki/US_DOD_5220.M)