

Obscene Images & Media

The Essentials

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 'obscenity'. Due to the nature of these types of offences and the fact charges often relate to the abuse of minors, there is considerable social stigma attached to this sphere of law, making it an area rarely discussed or debated.

The Act forbids the creation, showing, distribution, possession for showing or distribution, and advertisement of obscene media. Whilst the Act was originally developed to consider photographic images, it has been subsequently amended so as to include 'pseudo-images', artificial or computer generated images. Possession of such material constitutes an offence under the [Criminal Justice Act 1988](#).

To distinguish between child pornographic content, authorities rank material on a sliding scale of severity from one to five. This system is based upon the COPINE Typology¹ and ranges from semi-nude/nude photographs (level one) through to penetrative sexual assault (level four) and sadism or bestiality (level five). Sentencing guidelines² 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."³

In the United Kingdom the concept of 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 of tainted evidence and fundamental failings to corroborate 'facts'⁴, it remains an important case study for targeted police activity. To date Operation Ore has resulted in over three and a half thousand arrests, destroyed distribution networks and sent out a powerful message to those that might commit offences of this nature.

Digital Evidence

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 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.

¹ 'Combating Paedophile Information Networks in Europe' (COPINE) Project. Reference: www.copine.ie

² Sentencing Advisory Panel 2002. *The panel's advice to the court of appeal on offences involving child pornography*. London: Sentencing Advisory Panel.

³ 'Child pornography: an Internet crime', Taylor M & Quayle E 2003

⁴ Child porn suspects set to be cleared in evidence 'shambles', Times Online. Reference: www.timesonline.co.uk/article/0,,2087-1678810,00.html

It is important to note that computer forensic consultants that provide expert witness services in respect of obscene 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 obscene images have been deleted from the computer can an individual still be charged with possession?

R v Ross Warwick Porter⁵ 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. As a result, the appeal was held and it is now generally accepted that if an individual cannot retrieve or gain access to obscene content, then they cannot be regarded as having custody or control of it.

Can a forensic expert identify when a particular file was created or whether it was ever accessed, opened or modified?

Operations upon files and folders are recorded in 'timestamps', which provide 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 obscene media, timestamps provide crucial evidence as to actions and put into context when they occurred. A compelling defence case can be constructed if it can be shown that obscene media identified upon a computer has never been accessed/viewed.

Can images, which are essentially binary computer code consisting of 1's and 0', be considered obscene?

R v Fellows and R v Arnold (CACD Sep 1996)⁶ 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 obscene media. It was held that irrespective of format or transformations, if code can be reconstructed into material with characteristics that would liken it to an obscene photograph or movie, then for the purposes of the law that data would be regarded as obscene media.

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. R v Arnold married the technical and legal arguments, making it clear that

⁵ R v Porter (Ross Warwick) (2006) EWCA Crim 560

⁶ R v Fellows & Arnold (1997) 1 CAR 224

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 with obscene content 'popped up' on the screen un-requested by the user?

Many cases involving obscene images and media relate to the accessing of websites that have been confirmed to house illegal material. It has sometimes been suggested by Defendants that a specific website was not directly requested and simply appeared un-requested 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. 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, who was charged with breaking into computer systems owned by the American port authority in Houston⁷. 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.

The computer hard disk is second-hand – could the obscene media have originated with 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 such as US DOD 5220.22⁸, 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

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

⁸ 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

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.

Can Hash Codes, used to demonstrate integrity of evidence exhibits, be challenged?

Hash codes are the result of mathematical functions that allow the creation of unique serial numbers that are associated with specific files or file-systems. Should even the slightest modification of these files/file-systems be made, the serial number will change, highlighting the presence of revisions and that the integrity of the data may no longer be relied upon. Computer forensic investigators rely heavily on hash codes, particularly those created using the MD5 algorithm⁹, to show data integrity and match copies of images from one source to another. However, recent research has identified sophisticated attacks¹⁰ that, whilst highly technical in nature, show that under certain circumstances it may be possible to modify data and not affect the resulting hash codes. From a legal standpoint this raises the possibility that digital evidence exhibits could be tampered with and the modifications go unnoticed.

Did you know?

In software piracy cases involving the creation of copyrighted material, careful analysis of the computer can reveal how many times a ‘ripping application’¹¹ (program used to clone DVDs) has been run.

The Home Office is currently consulting on possible activation of provisions contained within Part III of the [Regulation of Investigatory Powers Act 2000](#) that would empower authorities with the right to force the disclosure of encryption keys and passwords from a suspect that has taken steps to secure digital information and files.

Find out more...

- [Introduction to the COPINE Typology](#)
- [Forensic Analysis of Internet History](#)
- [Internet Watch Foundation \(IWF\)](#)

⁹ ‘What are MD2, MD4, and MD5?’ RSA Security. Reference: www.rsasecurity.com/rsalabs/faq/3-6-6.html

¹⁰ ‘How to break MD5 and other Hash functions’, Xiaoyun Wang & Hongbo Yu

¹¹ Magic DVD Ripper. Reference: www.magicvdripper.com