Clause 53 of the Sexual Offences Bill

The problem of "making"

In the Protection of Children Act 1978 (PCA) Parliament created a series of offences which relate to indecent photographs of children, viz: s1(a) "taking" and "making", s1(b) "distributing" or "showing", s1(c) "possession with a view to distribution", s1(d) "publishing an advertisement". A "child" includes someone appearing to be under 16 and "indecent" implies some sexual element.

To a large extent these offences are similar to those applying to adult pornography, though the test there is the rather stronger one of "obscene". In both cases the aim is to criminalise the commercial aspects of the trade and (in 1978) the end-user "punters" committed no offence by mere possession.

Not that there was ever much doubt, but the "*R v Fellows and Arnold (1996)*" case established that electronic files (JPEGs, GIFs etc) count as photographs and therefore images from web pages, or the Internet generally, can be illegal. There was also a tightening up by the Criminal Justice and Public Order Act 1994 (CJPOA) to include "pseudo-photographs", viz: images created by graphics software from disparate elements that are not images of particular children at all.

So far, straightforward! However, back in 1988 Parliament had decided that "child pornography" was so heinous a thing that they would criminalise mere possession and hence in s160 of the Criminal Justice Act 1988 (CJA) a new offence was created. When illegal images were found, there was now no need to prove (as in PCA) any intention to distribute. The offence is one of "strict liability", viz: proving possession makes you guilty. However, there are some statutory defences decided "on the balance of probabilities" which include "legitimate reason", and that the material was received without "prior request" and it not kept for an "unreasonable time".

In 1988, being found guilty of the new possession offence would mean a fine, but being found guilty of the "making" offence could mean prison. In the CJPOA 1994 legislation the maximum penalty for "possession" was raised to a 6-month jail term and the maximum tariff for "making" to 3 years.

However, the police and CPS began to charge people who had only downloaded illegal images from the Internet with the higher tariff offence of "making". The argument ran that a copy of the image had been created on the suspect's computer and this creation met the tests of the "making" offence. Besides fitting the authorities' view that those convicted would face a "proper" sentence, the offence was serious enough to make it an "arrestable offence" and this simplified the process of searching a suspect's house and seizing their computer.

In 1999 the Appeal Court in three cases (*Bowden*, *Atkins* and *Goodland*) upheld the view that "making" did not only include pressing the button on the original camera, but also copying an existing photo or just saving a file to disk. This came about because the PCA did not actually define "making" and so the court used the normal dictionary meaning, despite the technology involved being very different from that which Parliament would have been aware of in 1978. In 2002 in the *Westgarth Smith,*

Jayson case, the Appeal Court ruled that voluntary browsing through indecent images so that they appeared, even momentarily, on the screen was also "making".

Meanwhile, Parliament had also come to the conclusion that the penalties for paedophile offences were too low, so in 2001 (after the publicity about the *W0nderland* case) "possession" went up to 5 years and "making" to 10.

The Sentencing Advisory Panel noticed the problem that the case law (*Bowden* etc) had created and in an advice document of 10 May 2002 they said:

http://www.sentencing-advisory-panel.gov.uk/c_and_a/advice/child_offences/page1.htm

"23. ... the downloading of indecent images onto a computer for personal use should be treated, for sentencing purposes*, as equivalent to possession, despite the Court of Appeal's decision in Bowden that someone who has downloaded such an image may properly be convicted of 'making' an indecent photograph under section 1(1)(a) of the 1978 Act. Our reason for this was that 'making' in the sense of making or taking an original indecent film or photograph of a child is clearly a more serious matter than downloading an image from the Internet, which is more akin to buying a pornographic magazine from a shop or mail order service."*

Now clearly this sentencing advice is somewhat makeshift, and fixing the legislation might well be preferable. In particular, attention must be paid to the difficulty that the current working definition of "making" is causing to system administrators, ISPs, the IWF, the police, prosecuting attorneys and defence experts. This difficulty arises because there are currently no statutory defences of "legitimate reason" (or similar) to the charge of "making". This lack of statutory defences made a lot of sense when "making" involved the clicking a camera shutter pointing at a live subject, but the case law has given us a very much wider practical meaning.

The current framework for dealing with reports of illegal images of children on the Internet dates from a 1996 agreement ("R3") between Government, police and the Internet industry. The industry funds the "Internet Watch Foundation" (IWF). The IWF operates a "hot line" for members of the public and assesses material. If material reported to the IWF is adjudged illegal then the hosting ISP is informed along with the police. Sometimes the public reports the images to the ISP who then passes valid reports along to the IWF for them to assess and act upon.

The difficulty is that with the broadly drawn definition of "making" almost all stages of the reporting and evaluation process can be seen to involve an illegal action. In particular ISPs have consulted their lawyers and have learnt that they would be committing an offence by:

- forwarding images to the IWF
  involves making a copy within their email systems
- checking out the images themselves
  involves intentional browsing
- or, preserving evidence for the police
  involves making a copy for later collection.

This has led to various forms of nonsense, for example the IWF developed a working practice such that when a website was reported to them they would tip off the police and only 48 hours later would they tell the ISP. This meant that the police had time to

make their own copy of the website contents, which the ISP might possibly refuse to do, but the harmful material remained available to the world for an extra two days.

Of course the IWF also do their own copying, browsing and such – indeed far more than any individual ISP. So far, they have relied upon the need for prosecutions to be authorised by the Director of Public Prosecutions (DPP) who usually delegates this to the Crown Prosecution Service (CPS). Since the IWF is well known to (and well respected by) the police and the Government (ministers regularly commend its work) there has always been felt to be no practical risk. However, ISPs, who may from time to time offend Government or police by their stance on unrelated matters such as data retention or competition issues might well take a rather less sanguine view.

Lobbying by the IWF and ISPs has led the Government to bring forward two protective mechanisms in s53 of the Sexual Offences Bill to address this issue of legitimate handling of paedophile material. One mechanism is that it is "necessary for the purpose of criminal proceedings" and the second is a formal "authorisation".

The authorisation scheme is clearly intended for bodies such as the IWF or for defence experts in a particular trial. For these cases the scheme is, in my view, completely uncontroversial, though one would expect to see the Association of Chief Police Officers (ACPO) bringing forward guidelines as to when authorisations are to be issued and what conditions are to be attached to them. ACPO might perhaps mandate the use of secure safes for removable media and encryption of hard disks to avoid problems if the computers being used are stolen.

The "necessary for the purposes of criminal proceedings" exemption looks at first sight as if this might be suitable for making a copy of a website for the police to later collect as evidence, or sending a suspicious image to the IWF for them to decide if it is illegal. However, when no criminal proceedings have yet commenced (because the police are not yet involved, let alone identified a suspect and considered whether to charge them) then this defence will not apply!

Perhaps, it is suggested, the police could issue ad hoc authorisations to cover the activities of ISPs who receive a complaint and investigate. This is problematic because of the speed at which authorisations would be needed, and because it may turn out that the image, although disturbing, is not illegal and so it would be a waste of police time to be involved at all. This often happens with photos of young adults who turn out to be over 16 (or in future 18) and so there is no offence. Alternatively, the photos (perhaps of smiling babies) are, because of the context in which they are made available clearly meant to be for paedophiles and hence are reported, yet the actual images are not "indecent" and hence unlawful – in another context, a family photo album, they would be unremarked upon. Clearly ISPs will be cautious about concluding images are legal and will often consult with the experts at the IWF, nevertheless, they do play a role in filtering out inaccurate reports.

Thus, having Chief Constables issuing authorisations in response to events that may turn out to be of zero interest to the police would be a heavy burden, yet relying on authorisations being issued retrospectively clearly suffers from exactly the same problem as the current scheme of refraining from prosecution. It requires the ISP to

take their immunity on trust, and their legal advice would be to be more prudent and avoid the issue by deleting evidence or refusing to filter out inaccurate reports.

Authorisations issued prior to the event, "in case something happens in the future", would also be a significant burden on the police. There are believed to be over 700 organisations that are "ISPs" in the UK and ACPO would need to develop complex procedures to ensure that these companies received the authorisations they needed, perhaps at several different sites coming under different Chief Constables. Since the Chief Constables would be wary of handing out "licenses to surf" to individuals of whom they knew little, they would clearly wish to minimise the number of authorisations that were made available. Of course if an ISP failed to receive such an authorisation then this would signal that they would face certain prosecution for any "making" offence and they would be most unlikely to co-operate in handling material or preserving any evidence at all.

So far, the discussion has been cast in terms of ISPs because their role in dealing with paedophile material is well understood and well documented. However, their number is very small indeed when compared with the number of individuals doing system administration (sysadmin) tasks in schools, universities, medium and large size companies. These sysadmins are routinely involved in dealing with complaints about inappropriate use of computers and networks and will be routinely examining content to determine if it breaches company guidelines. Where the material turns out to be illegal images of children, and regrettably that does occur occasionally, then obviously the sysadmin will call in the police to investigate.

Like the ISPs, the sysadmins are rapidly becoming aware that they too have broken the law by "making" an image during the course of their examination and they are only relying on the good will of the DPP and CPS not to be prosecuted. As with the ISPs this will surely tend to reduce reporting and co-operation, and the very large number of situations, people and organisations involved make almost any scheme involving authorisations look completely impractical.

So that's the, rather complex, background – what are the public policy issues here?

Firstly, the police units and the IWF who will regularly handle large amounts of illegal material and so on need to be properly authorised and technical and organisational standards adopted to ensure that the material in their hands does not get further distributed. Authorisations backed by an ACPO Code of Practice with strong teeth are clearly the way forward for this group.

Secondly, ad hoc investigators who are involved at the start of a case should be protected from the threat of prosecution for taking copies of material for evidence purposes or for reporting apparent crimes to the authorities.

Thirdly, it is necessary to ensure that paedophiles cannot use the defence of "I was about to report this to the police" to avoid prosecution. This will necessarily involve continuing to criminalise "vigilantes" who purposely look for illegal material in order to report it. It is also necessary to ensure that sysadmins who are permitted to view material in the earliest stages of an investigation should not thereby receive a "get out of jail free" card if they view illegal material in another context.

I believe that the best way of dealing with the second and third objectives is to change the definition of "making" so as to avoid catching "incidental copies" made in the course of viewing material. The notion of "incidental copies" is already widely used in discussions about copyright, and "caches", and encapsulates the idea that the technology requires some automatic copying in order to function.

The ad hoc, first-line, investigators would continue to be guilty of the "possession" offence but they would be readily able to avail themselves of the statutory defence of "legitimate reason" which is already in CJA 1988. If the police and CPS are not convinced that the activity is legitimate then the courts can consider the facts and decide. Paedophiles will not be able to use this defence improperly because their reasons will always fail to be "legitimate".

If Parliament is not prepared to tackle the definition of "making" then this is not the *only* way to meet the public policy objectives I have identified. It would be possible to add statutory defences for "making"; it would be possible to extend the proposed exemption for criminal proceedings to include all circumstances when they might reasonably be expected to occur; or indeed it might be possible to develop the large scale authorisation scheme that sysadmins and ISPs would need. Overall, though I do think that it would be simplest for Parliament to undo the effect of the case law in Bowden etc (which the Sentencing Advisory Panel has already negated) and redefine what the elements of the offence of "making" actually are.

SUMMARY: s53 authorisations are fine for making the IWF's activities lawful but are unsuitable for the many sysadmins and ISPs who are often the first investigators of reports of illegal material. Case law has created a broad definition of "making" and the lack of statutory defences to this offence make every investigation illegal. A simple fix would be to redefine "making" to exclude incidental copies. Investigating sysadmins would remain guilty of "possession" but would be able to put up the statutory defence of "legitimate reason".

I apologise for such a long briefing on what might be seen as a trivial point in a complex Bill. I would be pleased to answer any questions or expand further on any unclear points.

Richard Clayton, FIPR
07887 794 090, richard@fipr.org