

Pornographic Material

- Not Just an Internet Problem



Andy Churley from PixAlert, a company that specialises in preventing illegal and pornographic images, comments on proposed new Government legislation

Home Office Minister Paul Goggins recently announced that the Government intends to ban the possession of extreme pornographic material. Under the Government's proposals, it would be an offence to possess images depicting scenes of serious sexual violence and other obscene material.

This comes in part as a response to campaigners such as Liz Longhurst, whose daughter Jane was murdered two years ago by a man who was obsessed with violent porn on the Internet. For a long time they have been calling for violent pornographic sites to be taken down but since most of the sites are hosted outside the UK this would be impossible to enforce. The new legislation proposed by the home office turns its attention to the people who are actually downloading the material from the Internet.

But a common misconception is that most of this activity goes on in homes. Yet, according to the Society of Human Resources Management, 70% of internet porn traffic occurs during working hours. There is clear evidence that many people are spending time at work looking at illegal or pornographic images and that the activity can become addictive.

And it can happen anywhere. It recently hit the news in New Zealand that following an audit; a staggering 20% of the capacity on the country's police computer systems was being taken up by porn. In an investigation, some of these images were classified as 'objectionable' by the censor's office and could lead to a five year jail sentence.

In the UK, results of a recent survey of 400 public sector organisations by the public spending watchdog the Audit Commission, found a 16% increase in cases of staff accessing pornography and that inappropriate material now accounts for almost half of all incidents of computer misuse. In one publicised case last year at the UK Department of Works and Pensions, 2 million pornographic images were found on the network and even more worryingly 18,000 illegal images, leading to a series of dismissals, disciplinary action and prosecutions. With the potential new classification of illegal material this

figure may well have been even greater.

Existing legislation in the UK is clear – company directors and the managers they appoint can be held personally liable if negligence is found in the management of data and images on company computers. Neglect is defined simply as a failure to take appropriate steps to prevent an incident happening. Prosecution can be carried out under various pieces of legislation including Child Trafficking and Pornography Acts, Sexual Offences Acts, Obscene Publications Acts and Civil and Human Rights Acts. Yet a recent survey conducted by PixAlert and The Chartered Institute of Personnel and Development, over 50% of managers were unaware of this Risk.

While the main focus of the proposed new legislation is on cracking down on new material being downloaded from Internet sites, illicit images are already common on desktops and networks and there is a myriad of ways they can get there. Typically, a computer will have conventional points of entry such as CD/DVD. Ethernet card, serial and parallel ports. Now new modern connectivity protocols such as USB and Firewire have opened up computers to multiple new hardware devices with very high data transfer rates. New generation digital devices such as USB keys, digital cameras, mobile phones, discs, MP3 Players, portable hard disks and unsecured wireless networks are now commonplace and a breeding ground for distributing and storing porn.

The ability to plug and play using USB and Firewire has meant an extremely rapid introduction of digital devices such as USB keys, digital cameras, mobile phones, discs, MP3 Players and portable hard disks that are very hard for companies to monitor and control. Unmonitored laptop activity out of the office is also now widespread – a situation that is made worse with unsecured wireless networks.

In the survey carried out by PixAlert and the CIPD survey, an alarming 68% of companies said that they have not deployed a desktop technology to counteract these increased threats.

Many organisations that want to protect themselves from the effects of illegal and inappropriate content have simply

deployed web filtering technology at the gateway with a list of prohibited sites. All web traffic is filtered and access is denied to anything on the banned list. One clear problem with this method is that the dynamic nature of the web means it is impossible to keep a complete and up to date list of harmful sites. Furthermore, these standard web filtering methods can easily be by-passed through the use of secure Internet proxys, embedded content and file encryption.

While this proposed new Government legislation will help further raise awareness and help deter this unacceptable behaviour, the only way to reduce corporate exposure and stop illicit images in the workplace is by monitoring what people are actually looking at on the desktops and auditing corporate IT assets in order to find and remove legacy material.

There is no doubt that the proposed new legislation is a positive step and could be a useful deterrent but this needs to be combined with greater awareness and use of preventative technologies, particularly in the workplace. In particular, it is important to recognise that the key issue is in the nature of the content ... not where it was accessed. This is not just an Internet problem; pornographic and illegal images can originate from many sources.

Andy Churley (BEng, CEng, MBA, CITP, MBCS) is marketing director at PixAlert, www.pixalert.com

PixAlert International
Digital Hub
10-13 Thomas Street
Dublin 8, Ireland

Tel: +353 1 707 8860
Fax: +353 1 707 8861
Email: info@pixalert.com

