

PRESS RELEASE

Release date: 20th February

Are non technical juries keeping criminals at large?

In England and Wales the only qualifications required of a jury member to be eligible to appear in a court of law are that they are registered on the electoral roll, aged between 18 and 70 and have lived in the UK for at least 5 years. Jurors are not required to hold any professional qualifications and there are to date no technical jury qualification guidelines for cases involving complex computer data. Where does that leave us then, when vital yet highly complicated technical information needs to be communicated and thoroughly understood in order to fairly evaluate a case? Let's take a look at the evidence....

Computer and digital evidence has naturally entered the UK's courtrooms on an enormous scale as we enter a predominantly digital communications era thanks to the likes of chat rooms, emails and mobile phones. This combined with the introduction and amendments to legislation such as the Data Protection Act 1998, Criminal Justice Act 1994 and Protection of Children Act 1978, has generated a new wave of criminal offences that demand digital evidence in order for successful prosecution. This evidence, presented in what are often serious and expansive cases such as the international Operation Ore investigation into child abuse images, can contain highly complex and technically advanced information.

In many instances, defence in such cases rests on the precise way in which data has arrived onto a computer. Take for example a case involving indecent images such as Operation Ore - were the graphics simply viewed or downloaded? Had the defendant actively sought to discover them or were they sent maliciously to the machine? Uncovering these data trails can be a deciding factor in criminal cases. Additionally, in the majority of cases data will have been deleted or moved about as the offender attempts

MORE

to cover their tracks, and so not only is the trail a complicated one, it is often deeply embedded within data which only becomes visible under forensic investigation.

Aside from the newly categorised ‘cyber crimes’ (identity theft, hacking, theft of intellectual data etc) there are the more traditional offences such as drug trafficking and money laundering that can be aided by computer forensic evidence. It is surprising how many criminals keep detailed spreadsheets of their finances or attempt to fabricate emails in order to back their defence. The war against the ‘Happy Slapping’ culture for example can also be fought with the help of recovered media files from mobile phones. Nothing is ever permanently deleted, digital fingerprints (known in forensic circles as ‘MD5 hash values’) and trails of evidence are resilient.

This is precisely the stage at which the understanding of digital evidence, its forensic recovery and communicating the methods taken in court to a non-professional, non-technical jury becomes problematic. The investigation, interpretation and presentation of evidence that is often derived from binary data is highly complex and usually littered with technical terms and concepts – is it being handled carefully enough in court or is it falling on deaf ears when presented to a jury?

“I think the courts can seriously underestimate the sheer quantity of information that computer based evidence can consist of – one hard drive could contain hundreds of thousands of files. This combined with the complexity of the information being heard, alongside any potential discrediting of the data by opposing counsel, can devalue what is actually often damning evidence” says Joel Tobias, Managing Director of computer forensic company CY4OR.

Generally speaking, evidence collected by a reputable computer forensic company, acting independently or on behalf of law enforcement agencies, can be relied upon; the ACPO Good Practice Guide and stringent security checks of premises and staff ensure this. From this angle at least, if secured correctly digital evidence can be taken at face value.

MORE

Legislative guidelines such as ACPO are addressing the secure collection of computer forensic data, however the driving force behind a change in legal practice relating to IT cases appears weak. The British Computer Society are however one organisation in particular that are energetically voicing their proposals for change;

“The BCS wishes to participate in the continual change to, and interpretation of, the law and the processes of investigation and prosecution to take account of the increasing use of computers in society.”

“IT systems today are international and we remain concerned that there are too many inconsistencies in the law, processes and procedures between jurisdictions. This may allow criminals to remain at large. We therefore support greater international harmonisation of laws on eCrime and the processes for addressing all crimes committed in a computer environment.”

Is it indeed now time to implement a sensible selection system of jury members for IT related cases, who themselves have technical backgrounds or who have received comprehensive training in these matters prior to trial?

Joel Tobias from CY4OR continues “I think it is fair to suggest that the majority of the legal system as a whole is still unprepared to deal with the issue of computer based evidence – we try to offer a friendly matter of fact approach in our advice and reports so that communication and understanding between the legal industry and ours is as comprehensive as it can be.”

0161 797 8123

info@cy4or.co.uk

www.CY4OR.co.uk

ENDS...

Carrie Moss

0161 797 8123

Carrie.moss@cy4or.co.uk

NOTE TO EDITORS

If you would like to sample any part of this release do please let Carrie or any member of the CY4OR team know.

PO Box 439, Bury, Manchester

Copyright 2006 CY4OR