

ST JOHNS BUILDINGS CRIMINAL LAW SEMINAR

INTERNET & COMPUTER CRIME

NOTES TO ACCOMPANY SLIDE PRESENTATION

3

Real-world criminal offences such as forgery, fraud, deception, copyright theft often use computer technology to facilitate. For example the creation of false documents.

The Internet (and therefore computers) is increasingly the medium through which crime is perpetrated: identity theft.

Criminal acts may also be directed against computers, hacking into computer systems for information or destructive purposes such as unlawful modification of computer. Prosecution of a school computer assistant who when dismissed at the end of term left a 'time bomb' on the school computer that was activated when the newly employed staff member started up the computers at the beginning of the new term. The program caused all data files to be deleted.

4

Fabricating documents: currency, passports, insurance certificates, train tickets (recent case: computer expert avoided £12,472 in train fares over two years by printing his own tickets).

Internet banking is used to launder money without ever entering a bank.

5

Email Scams: Nigerian wants to bank £1 million in your account. Obtaining credit card details by bogus 'your account has been suspended, click here to reactivate,' emails.

Cyberstalking: threatening emails

Bogus webchat identity: has been used to lure children into sexually explicit conversation. One case adult male pretended to be a teenage girl, putting up 'live' footage of the girl and encouraging two young boys to undress and perform sexual acts on each other. A similar procedure can be used to fool people into revealing personal details, including address, or to meet up for a sexual encounter.

Email harvesting: Programmes that enable the Internet to be browsed for email addresses that are then used to solicit information from the email address owner.

Hacking into Internet Bank accounts: Nicholas Sarkozy's bank account recently hacked.

Use of stolen credit card details to make online purchases or transfers of money. Provide the account is in credit and the account number is correct the transaction will be processed.

6

Computer crime can be carried out across international borders, causing difficulties over jurisdiction and differences in law of the relevant countries. Phishing is a method of tricking people into disclosing personal information for the financial gain of the offender.

When I checked the source of this email I found it originated from an Illinois College faculty member called Porkchop, in Jackson Florida with a website called Sikh Answers.com. According to the site logs, he has had more than 10,000 hits on the website - people submitting their bank details!

In 2008 fraudsters were able to insert a phishing page on a home office website page, directed at users of an Italian bank.

Phishers can also display a genuine website but impose a pop-up on top of the genuine site in the background.

The 2006 Fraud Act closed loopholes in fraud offences, where prosecutions would have to be conspiracy to defraud or obtaining property by deception. Under the act possession of any software or data for use in a fraud could result in a prison term of up to five years. The Act also provides that writing software "knowing that it is designed or adapted for use in ... connection with fraud" can result in a sentence of up to 10 years.

7

Came into effect 15 January 2007. The Act gives a statutory definition of the criminal offence of fraud, defining it in three classes - fraud by false representation, fraud by failing to disclose information, and fraud by abuse of position. It provides that a person found guilty of fraud was liable to a fine or imprisonment for up to twelve months on summary conviction, or a fine or imprisonment for up to ten years on conviction on indictment.

If not possible to deceive a computer, how could it apply to computer fraud? Can a computer be deceived? Online frauds are now a major concern.

Problems of deception are now overcome by Section 2: dishonestly making a false representation knowing that the representation was or might be untrue or misleading with intent to make a gain for himself or another, or to cause loss to another or to expose another to a risk of loss. A representation can be made to a machine, eg ATM. It is not relevant whether the false

representation is believed or has any effect on the recipient. For the purposes of s2 a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention).

This covers phishing¹ & pharming²: but is also covered by s3 of the CMA 1990: unauthorised modification Re Yarimaka (2002) EWHC 589 sending email pretending to be someone else that email enters the computer, is a modification which is unauthorised, with intent to modify the contents, and the reliability is impaired, because contains inaccurate information.

Possession of an article for the use of fraud and the making or supplying of such articles are now an offence (ss6 &7)) but Porter still applies, document can only be in possess if knows he has it or has access to it.

8

Causing unauthorised modification of computer under the Computer Misuse Act 1990, maximum penalty set to be increased from 5 to 10 years. Usually prosecuted using computer crime legislation. Barak Obama's campaign computer system hacked.

Botnet and zombie network: uses compromised computers to

Drive-by downloads: indirectly authorised downloads by the user without understanding the consequences, or happens without knowledge.

Wireless sniffing of keyboard strokes from distance (65 feet)

Using unprotected or poorly protected wireless network of another to download illegal material such as child pornography. (Show Screen shot of Wifi Radar Screen).

A Denial-of-Service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. The attacker floods the webserver with messages endlessly repeated. This ties up the system and denies access to legitimate users. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways. One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered

¹ In phishing, the perpetrator sends out legitimate-looking e-mails, appearing to come from some of the Web's most popular sites, in an effort to obtain personal and financial information from individual recipients.

² Pharming is a scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent Web sites without their knowledge or consent. Pharming has been called "phishing without a lure."

effectively unavailable. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

Covered by s3 CMA: there is no need for any modification to have occurred and (3) the impairment can be temporary. In the mail bombing case of **R v Lennon [2006] EWCH 1201, 11 May 2006**, the Divisional Court stated that, although the owner of a computer able to receive e-mails ordinarily consents to the receipt of e-mails, such consent did not extend to e-mails that had been sent not for the purpose of communicating with the owner but for the purpose of interrupting the operation of the system.

9

Amended by Police & Justice Act 2006 (not yet in force) to include new offence of making or supplying of articles for use in CMA offences (s3A) (But could also be an offence under Fraud Act 2006).

See section 17 for definitions.

Note that there is no definition of a computer!

Unauthorised access: Causing a computer to perform any function with intent to secure access to any program or data held in any computer. The access must be unauthorised and he knows that is the case. Was summary offence only, now either way (2 years). Amended to include the use of one computer to secure unauthorised access to another. Requires knowledge that unauthorised and intent to obtain information about a program or data held in a computer.

Access defined: causing a computer to perform any function he alters or erases the program or data, or copies or moves it to any storage medium, uses it, or has it output from the computer in which it is held, including by displaying, or in any other manner.

R v Mark Hopkins [2007] website designer hacked into competitor website. 5 months suspended 2 years.

R v Daniel Cuthbert [2005] IT consultant donated £30 online to charity and then checked the site security. Fined £400.

Several cases of police officers using PNC for unlawful checks.

Access with intent to commit further offences (s2): The above offence with intent to commit an offence (with a maximum fixed by law or minimum term 5 years for adult), or to facilitate the commission of such an offence whether by himself or by any other person, even if the further offence is impossible. Either way offence: 5 years.

Unauthorised act with intent to impair (s3): Any act which causes an unauthorised modification of the contents of a computer and has the intent to impair the operation of the computer, prevent or hinder access, impair operation of programme or reliability of data. Requisite knowledge: knowledge that any modification intended is unauthorised. Immaterial whether the modification is or intended to be permanent or merely temporary. Either way offence: 5 years. Covers DoS attacks.

Modification is defined as by the operation of the any function of the computer any programme or data is altered or erased, or program or data is added to its contents. Any act which contributes to such a modification shall be regarded as causing it (s17(7)).

R v Alfred Whittaker : software developer installed time-lock into software that denied access to the software after a dispute arose over unpaid fees.

The above offences need not be directed any particular programme or data or any particular computer.

R v Delamare [2003] bank official paid £100 to access account details (4 months)

R v Lindesay [2002] revenge attack by freelance computer consultant using knowledge of former employer's system, £9,000 damage. (9 months).

Re Yarimaka (2002) EWHC 589 entering false information into a computer by email, is a modification which is unauthorised, with intent to modify the contents, and the reliability is impaired, because contains inaccurate information.

R v Raphael Gray [2001] teen hacker found security weaknesses in e-commerce website and accessed 23,000 credit card records. Used Bill Gates credit card to send him some viagra. 3 years probation and medical treatment!

10

These key concepts are essential to understand cases involving computer and Internet crime: some may provide or eliminate defences.

11

Care has to be taken with examination of computers. In **R v Moody** an IT specialist was accused of accessing remote maintenance of a LA computerised telephone system. Outgoing calls could not be made and all incoming calls routed to one extension. At voire dire, evidence of files seized from forensic image copy of the hard disk. But files had been corrupted by previous police examination. Indictment stayed.

12

It is essential that before the case is pleaded all relevant material has been

disclosed. Analysis of the evidence by a police expert is not a substitute for the core evidence. Where a computer has been seized and there is to challenge as to the contents, a copy of the hard drive (mirror image) can be produced in minutes. If it contains illicit material (eg child pornography) a copy will not be supplied but the Defence must have access to the material to examine, if required.

Check what software or level of expertise was required to find the material on the computer - it may be beyond the Defendant's ability to access.

13

It is not necessarily the case that the Defendant's computer is the one that has been connected to the Internet and used criminally. A wireless network may be used by others nearby, giving the impression to investigators that illegal use was by the Defendant. Open networks even if names are hidden are particularly vulnerable, but software programmes can search for likely wireless network passwords.

14

This is a common route for the distribution of child pornography. These programmes, such as Limewire, are designed to share by hidden default and download to a default folder. Internet filesharing of copyright material is also illegal but generally pursued by civil action for damages. Most actions have been against those sharing files to others and not those who have received the files. However filesharing is also dangerous, in that spyware can be downloaded without the user's knowledge. A common defence claim is that the files were downloaded without knowledge - can usually be disproved by location of stored files.

It is often argued that the user was searching for illegal or not criminal material, such as copyright music or adult pornography and that a batch of files or images were downloaded and when the user realised what it was deleted the file.

R V Dooley [2005] EWCA Crim 3093: charged with possession of indecent images with a view to distribution (S1(1)(c)PTCA 1978: 4 images in a file-sharing folder. Downloaded there by default and he normally moved images to folder not accessible to other file-sharers. Held distinction between 'with a view to' and intend to. If in that folder to enable others to see or download by access to that folder, that is with a view to.

Data protection (Processing of sensitive personal data) Order 2006: allows card issuers to process sensitive information supplied by law enforcement agencies so they can withdrawn card used to commit offences.

15

An unprotected computer connected to the Internet will be constantly probed for attack and installation of spyware.

R v Aaron Caffrey [2003] DoS attack that crippled the port of Houston, Texas. Came from teenager's PC. Acquitted on a Trojan defence - other hackers had taken control of his PC using a Trojan Horse virus. In an effort to rebut the defence the prosecution pointed out that no trace of a trojan horse program had been found on his laptop. However the defence countered that it was a self-erasing trojan, so no trace would be found. Jury believed the defendant, who was in effect his own expert witness. If this Defence is raised, the prosecution have the burden to knock it down proving that the defendant was responsible and not some other person - proving a negative. Jurors are more likely to believe that computers can be controlled by others as it feeds a conspiracy theory suspicion we all hold of technology.

The defence can be self-set up by a defendant installing a trojan himself to be 'discovered' by police or defence investigators. Prosecution experts do not routinely look for the existence of malware that may account for the downloading.

It is a not-uncommon plea that another computer user downloaded the offending images on the Defendant's computer. Unlikely, but possible. Prove that spyware is installed on the computer and look at times of download. Also need the IP address. Can be used to obtain information from the computer, eg mirroring keyboard strokes, or accessing personal files, but also can cause a target computer to access illicit material which is then shared onwards. Most defences can be knocked down by examination of the file location and file information.

Trojan horse is malware that appears to provide a desirable function but in fact facilitates unauthorised access to the user's computer system. As they are not self replicating, they are distinguished from viruses and worms, which are. Trojans require interaction with a hacker to fulfil its purpose. Purpose to allow a hacker remote access to a target computer system. Can do a number of things: upload, download files, keystroke logging, data theft, use the machine as part of a botnet, viewing the user's screen,

In August 2008 South Australian police arrested a 20-year old man on charges of infecting 3000 computers worldwide with Trojan malware capable of capturing banking credentials and credit card information from compromised machines. The remote machines were used to do the collecting and then pass the details back to the Defendant.

Spyware, and remote programmes to obtain private details from a targeted computer:

- i. Keyboard tracker, sends details of keystrokes to a remote location
- ii. Wireless sniffing of keystrokes now possible with wireless keyboards.
- iii. Access to files on your computer, even capturing screen.

16

When a computer connects to the Internet, the Internet Service Provider (ISP) assigns an IP address. In addition, all web servers and websites have unique IP addresses associated with them, allocated by the ISP. Users with a computer connected to the Internet can ping other IP addresses to see if a remote system is active or if they can connect to it.

An internal network will assign out IP addresses to individual computers to identify them on the network (usually begins 10). Most network computers can be set to use the same IP address when connecting to the Internet.

An IP address can be detected for any computer connected to the Internet. It can then be traced back to the ISP and then the customer.

The long number is St Johns Buildings IP address, slightly altered for security reasons.

17

This is the long header of an email. It is normally hidden from view but it shows the route the email took to get to its destination.

A search of the IP addresses in the above email told me that the Internet Service Provider is Fused Networks Ltd and leased to St Johns Buildings Barristers Chambers (Manchester), that the computer was connected to the Internet by a cable or DSL line. It also gives me a geographic location for the computer, the accuracy of which depends on computer density. In this case chambers computers all appear to use the same external IP address.

That IP address can then be pinged to see if it responds - is it up and running?

A check on my own IP address gave me a location less than a mile from my home.

18

Each computer or other hardware device has a unique Media Access Control (MAC) address. This is nothing to do with Apple computers. It cannot be traced back from the Internet.

19

This is the most important information to look for: Where has the file been stored? Users often create custom folders. Pornographers tend to collect images in folder groups of type of images. If a file is in a default download folder it is more easy to argue inadvertent download.

Make sure that a check has been done on seizure of computer to see whether the computer's time and date are correct. This may be relevant to the Defendant's presence. Often a computer is out of sync with real time.

Any file has additional information attached to it that is time and date stamped. This includes the full file name and location in the computer but also the date/time the file was created, modified, and in many cases last opened. This can disprove inadvertent downloading or access.

However, if the file was downloaded to the computer and not created by that computer it may in some cases bear the same time/date information until opened. Thus the information may not be reliable.

20

When using the Internet programmes such as Internet Explorer are set by default to automatically store a copy of any image displayed on the web browser. This is stored in the cache folder and is hidden from normal use and user searching. The purpose is to be able to load the images from memory rather than downloading afresh.

This cache is like a reservoir that has files constantly flowing into it until full, then it deletes the oldest first, so that the most recent viewing can be accommodated in cache. By an examination of the cache it can be seen what has been viewed on the computer going back weeks if not months.

21

Thumbnails are reduced-sized versions of pictures, used to help in recognising and organising images, an index to the images. On a website the thumbnail image may be the only thing viewed by the user, unless he clicks on it as a hyperlink to a full-size image or another web page. If shown on screen it will automatically be stored on the computer by Microsoft internet explorer, without the knowledge of the user.

Even when the full image has been deleted, references to files or images may remain on the computer as a thumbnail image. It is not the image itself but (usually) a very low quality copy stored by default as a reference.

Many child pornography cases have been based on thumbnail images either as indecent images themselves or proof that indecent images have been viewed or stored.

The FBI has posted hyperlinks that purport to be illegal videos of children having sex and then raid the homes of anyone who clicked on the thumbnails (which in fact did not lead to illegal images). The evidence was used to obtain

a conviction of attempted download of child pornography.

22

No text

23

Passwords can be broken, eg by dictionary attack - a method of defeating a cipher or authentication by trying to determine the decryption key or password by searching and trying likely possibilities: systematically trying all words in an exhaustive list, derived list words from dictionary.

Brute force attack: tries every key alternative. People tend to choose short passwords (7 or fewer) single words found in dictionaries, or the same with a single or double digit appendage. Spam emails work the same way: message sent to every email address consisting of a word in the dictionary followed by the @ symbol and the name of a domain. Eg list of christian names. Best passwords and email addresses are long meaningless sequence of letters interspersed with numerals.

Can it be shown that the Defendant was the only one with access to the computer?

A computer may be password protected but if it is left on, then any member of the household may have open access. Web browsing programmes usually have protection settings, check if they are active. Passwords may be level controlled or only be needed for installing new programmes. Does the lock out screen come on if the computer is unattended?

Many people forget passwords so have it written down next to the computer - or in a file on the computer desktop.

These are important features to check when considering alternative users of a computer.

24

Encryption is the process of transforming information (referred to as plaintext) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as ciphertext).

25

Provisions in Part III of the 'Regulation of Investigatory Powers Act 2000' provide law enforcement authorities with the right to demand access to the original plaintext or encryption keys, so as to prevent crime or assist in ongoing investigations.

Does not have to be a defendant: only that believes on reasonable grounds

that protected information and disclosure is in the national security or economic interest, or for the purpose of preventing or detecting crime.

To obtain a section 49 notice for protected information, police forces must first apply to the National Technical Assistance Centre (NTAC) on the basis that they have reasonable grounds to believe. Although it appears to be part of the Home Office's Office of Security and Counter Terrorism, it is in fact located at GCHQ in Cheltenham. Following NTAC approval it then requires judicial permission (none refused). First notice issued was in relation to animal rights extremism. The two convictions were in relation to counter-terrorism, child indecency, and domestic extremism. 15 notices issued from 49 applications in 2008-2009.

Sentence would appear to be less onerous than a conviction for child pornography and sex offenders registration.

26

About 3,000 persons prosecuted annually for one or more of these offences.

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, 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. Sentencing Guidelines & Copine scale.

R v Porter (Ross Warwick) (2006) EWCA Crim 560, held: a person could not be in possession of indecent photographs of children under the Criminal Justice Act 1988 s.160(1) if he no longer had custody or control of the images. In the case of deleted computer images if a person could not retrieve or gain access to an image then he no longer had custody or control of it. Downloaded files had been deleted and the recycle bin emptied but examination found thumbnail images elsewhere. The larger images had been deleted and could not be retrieved by clicking on the thumbnail. The Defendant, without specialist knowledge and software, could not have accessed the thumbnails. On the charge of possession, it was clear that they had been deleted before the computer had been seized. Held: he couldn't be in possession if he did not have possession or control of the images. If at the time of the offence an image was beyond his possession he would be not guilty. It was a matter for the jury to decide on the basis of his knowledge. But he would have been guilty of possession at an earlier time and also guilty of the act of downloading. Care is necessary to include an indictment date to

cover the period when the image must have been on the computer.

Data protection (Processing of sensitive personal data) Order 2006: allows card issuers to process sensitive information supplied by law enforcement agencies so they can withdraw card used to commit offences.

27

R v Fellows & Arnold (1997) 1 CAR 224: The court held that a computer file containing data (a series of 0 and 1) that represented the original photograph in another form (and could be reconstructed from the code) is a copy of a photograph under Section 7(2) of the 1978 Act. It followed that downloading an indecent image from the Internet was making a copy of an indecent photograph, since a new copy had been caused to exist on the target computer. Each image viewed on a computer screen is not remotely looking at an image in another location but causes a new and identical copy to be created on the target computer. Hence this is a 'making' an indecent image charge.

Atkins v DPP (2000) making does not include unintentional copying to a cache folder. Cannot be guilty of possession if unaware of existence of a cache of images.

The only thing that may be different is the file information, which may have a different creation and viewing date and may have a slightly different name, particularly if there is already a copy of this image in the target folder location.

It frequently happens that multiple copies of images with the same file name are downloaded. In this event the computer usually denotes each new copy with a sequential number at the end of the file name: illegalimage.jpeg; illegalimage(1).jpeg; illegalimage92).jpg.

28

Section 160(2)(a) defence that not seen the image and did not know or have any cause to suspect it to be indecent, or c), send to him without prior request by him or on his behalf, and did not keep it for an unreasonable time.

Smith & Jayson: Not an offence of possession to open an email attachment containing an indecent image if unaware did or was likely to contain an indecent image. Deliberate downloading of an image from the Internet to the computer screen was an offence of making an indecent image, causing a new image to appear on the screen.

Also R v Collier [2004] it may be a defensible position in law to show 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 arises in cases involving indecent images on the Internet, when the web browser 'caches' (automatically saves copies of webpages and imagery to the local hard disk without any user intervention). Forensic examination of the computer may assist to prove viewing or absence of viewing or access to the indecent image.

In *Atkins v DPP* (2000) Dr Atkins, an English lecturer at Bristol University, argued that he had a legitimate reason for having indecent photographs in his possession for research. The court disagreed that it was honest research into child pornography. There is a defence of legitimate reason (section 160(2)) which is a matter of fact to be decided in each case. Genuine academic research would be a legitimate reason. However, ignorance of the operation of the computer cache or the existence of the cached images was not a defence.

29

R v Perrin: the Defence raised was that the Defendant was distributing his content via servers in a country other than the UK. The court held that 'downloading' material into the UK constituted 'publication' irrespective of where it was 'uploaded', and therefore was an offence under UK law.

R v Waddon: The court considered the question of "publication" on the Internet in the context of the Obscene Publications Act and held that this could occur more than once. Publication occurred when images were uploaded on to the web site by the website contributors and when the images were subsequently downloaded by users.

R v Skinner (2005): holds that even material automatically copied from one 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.

30

Can a child pornography image or website link 'pop up' on screen without user request? A common defence tactic is to suggest that a suspect website was not directly accessed but just appeared on the screen whilst browsing the Internet.

Accessing any pornographic sites may well provide links to indecent images of children. 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 further content than that displayed on the opened page. A 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 images potentially 'cached' and saved to the computer drive – without the knowledge or action of the user. Windows controls can be set to block pop-up windows from being displayed. Check if the control was activate.

Forensic evaluation 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. In most cases an Internet browsing history will reveal evidence of accessing websites that contain or relate to child abuse images. Google search terms may also reveal searches for such indecent images. In most cases this defence is undermined by the Internet browsing history.

THD was successfully used in child pornography case in **R v Julian Greene [2003]**. The computer dialled the Internet on its own and accessed a child porn site as a default homepage. Couldn't get rid of the virus. Expert examination by the Defence found 12 Trojan programmes. Case was discontinued.

31

Computer crime can be carried out across international borders (Nigeria million pound scam to use your bank account), causing difficulties over jurisdiction and differences in law of the relevant countries.

For example, American Express and Visa fraud using accounts of people from Israel, Brazil, Argentina, USA. After up to 7 weeks delay the customer reports that transactions on account statement not conducted by them. Amex investigation confirms fraudulently used but cannot provide evidence in acceptable format - no witness statement, just letter of complaint. Almost impossible to get evidence in acceptable format and then unwillingness of witnesses to give evidence, or the expense of doing so renders potential prosecutions impractical.

CMA 1990 has jurisdiction if there is at least one significant link with the domestic jurisdiction. R v Waddon [2000] CA, held that the content of US websites could come under UK jurisdiction when downloaded in the UK.

Difficulties when computers are purchased second-hand or hard-drives replaced with second-hand ones. Cannot prove download and unless can prove access, cannot prove possession.

Trojan Horse Defence has resulted in a number of cases being discontinued since 2003. Most computers have many viruses unless protected by up-to-date virus killer programmes.

THD was successfully used in child pornography case in **R v Julian Green [2003]**. The computer dialled the Internet on its own and accessed a child porn site as a default homepage. Couldn't get rid of the virus. Expert examination by the Defence found 12 Trojan programmes. Case was discontinued but not before he spent one night in the cells, 9 days in prison, a bail hostel for 3 months and lost custody of his daughter and possession of

his house.

Also **R v Karl Schofield [2003]** THD defence succeeded. Defence expert proved that TH existed on the computer, the day before the images were downloaded. He lost his employment and was targetted by vigilantes following reports of his arrest. Took two years to come to trial.

32

Jury IQ

- i. Cannot assume that jury understand how the Internet works;
- ii. But could jury questions be used to find a panel that has a basic computer knowledge?

Technical nature of terms and processes difficult to follow (show example of one jury trial where eBay bidding explained to the jury);

Problem of expert Witness incapable of explaining technical matters in layman's terms. Need to review this ability before engaging as an expert.

Diagrammes, powerpoints, can be used to and video clips to illustrate points. For example, animation of mouse moving over screen and clicking on items.

Trojan horse defences (THD) particularly difficult to rebut, because it requires the prosecution to explain some abtruse, technical concepts and processes to a lay jury in a way lay people can understand and can use that understanding to conduct a critical assessment of the THD presented to them. That can be a very difficult process; it will require not only expert witnesses, but the skilful use of graphics -- animations, diagrams, etc., -- that can really let jurors grasp what would have had to occur for the THD to be valid and why that did not occur (establishing, by inference, that the THD defence is invalid). Doing all that can be a huge undertaking for the average prosecutor, as it requires time, expertise and the money to pay for the creation of the necessary demonstrative evidence (animations, diagrams, etc.).

THD was successfully used in child pornography case in **R v Julian Green [2003]**. The computer dialled the Internet on its own and accessed a child porn site as a default homepage. Couldn't get rid of the virus. Expert examination by the Defence found 12 Trojan programmes. Case was discontinued but not before he spent one night in the cells, 9 days in prison, a bail hostel for 3 months and lost custody of his daughter and possession of his house.

Also **R v Karl Schofield [2003]** THD defence succeeded. Defence expert proved that TH existed on the computer, the day before the images were downloaded. He lost his employment and was targetted by vigilantes following reports of his arrest. Took two years to come to trial.

David MW Pickup

St Johns Buildings

16 Winckley Square

Preston

david.pickup@stjohnsbuildings.co.uk