**Scenarios/topics for methodology exercise**

|  |
| --- |
| **Case Study 1** Facts / scenario Bobby is a Police Officer. One night he is on duty and sees a Mercedes parked outside his house. He does not recognise the car but suspects that it belongs to his wife's boss. He phone’s into the police station and asks Mary the computer operator to tell him who owns the Mercedes saying that the car had just driven through a red traffic light. Mary confirms that the car does indeed belong to his wife’s boss.  *Has Bobby committed a criminal offence?*   * **Issues**   *Has Bobby accessed a computer system? Was that access without right?*   * **Points for discussion**   The computer was accessed by Mary not Bobby she has is authorised to access the data on the computer, she is innocent. It was Bobby who, acting through an innocent agent caused the data to be accessed. He lied to Mary (an illustration of social engineering) does this amount to access in law?  Both Bobby and Mary have the right to access the Police computer but subject to strict conditions relating to a legitimate query in connection with police activity. Where the access exceeds this authorisation does this constitute an offence?  What if Bobby goes into the police station and manages to look over Mary’s shoulder (shoulder surfing) whilst she is making a legitimate enquiry in relation to the ownership of the Mercedes?  The ‘shoulder surfing’ has resulted in Bobby gaining access to computer data. There may be a question as to his ‘intention’ and of course he has not manipulated the computer system in order to gain access but he has still obtained access without right (though this would be very difficult to prove).  This case study is designed to have delegates consider the question of authorisation (access without right).  The delegates could also be asked to consider the position had Bobby gone into the police station and looked up the information as to the ownership of the Mercedes on a card index system – the information being the same as that held on computer? The point here is that it is not the data itself that is protected (though that may be protected under other data protection legislation whilst Bobby’s misconduct might also constitute an offence) rather it is the medium on which that data is stored that is being protected.  Police computer systems hold vast amounts of personal information relating to individuals along with a lot of sensitive information. Access to such data should only be granted to those who have a legitimate interest in it. In the UK police officers and police computer operators are frequently found illegally accessing police systems for purposes of their own e.g. to find information that might be interest to the press or in the case of corrupt officers to discover what information is held on a particular person or whether a particular person or group are under active investigation. |
| **Case Study 2**   * **Facts / scenario**   A security guard at a bank is approached by a group of criminals who ask him to place a device known as a key logger onto the back of a number of terminals in the bank. The key logger records the keystrokes of the user and captures passwords and other information that would enable someone who had access to the terminal to log into the user accounts of bank staff.  An additional feature of the Key Logger device enabled it to record Skype phone calls made by the user of the terminal.  The criminals also placed a bug on the desk which picked up sound, including all phone calls made and received by the user of the terminal.  *Has there been an illegal interception?*   * **Issue**   *Has there been an interception?*  *Has that interception been achieved by technical means? Has data been transmitted to or from a computer system?*   * **Points for discussion**   The key logger is a technical device that is capturing data transmitted from the terminal. This amounts to an interception and is clearly without right.  What about the Skype calls? In this scenario it appears that the data travels on the same line as other data transmitted from the computer but what if the user had a stand alone Skype phone? Would such a phone constitute a computer system. The convention defines a ‘computer system’ *any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*; and ‘computer data’ *as any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*.  The use of the audio bug may be a little more difficult. Is it an ‘interception’? In the UK the courts have held that for an interception to have taken place there has to be some sort of interference or abstraction of the signal whilst it was being transmitted on the network, here the recording takes place independently of the transmission notwithstanding that the same information is obtained had the device been placed on the ‘line’.  What if the key logger was placed on the system by the Company who are anxious to ensure that their employees are not using the internet for an inappropriate purpose?  Most telecommunications systems travel on both public and private networks. At the point where the communication leaves your property it moves from a private system to a public system. The controller of a private system has the right to access communications using that system; so for instance, you would be able to monitor conversations on your home telephone line provided that whatever technical device you used in order to do so was connected to the private side of the system.  This scenario is designed to have the delegates consider each of the elements of interception, that there is an interception of computer data in the course of its transmission by technical means without right.  The delegates should be clear that this provision is designed to protect the contents of communications rather than information connected with the addressing of the message or the cost of the service. |
| **Case Study 3**   * **Facts / scenario**   A criminal gang communicate using a web based e mail system that can be accessed through the internet anywhere in the world. Rather than send each other messages that might be intercepted by the police or which may incriminate them if found on their computer they use a ‘dead letter drop’ system. What they do is write their message as a draft which is never sent, other members of the gang have the password which enables them to access the e mail account and read and respond to the message.  If the police were able to access the draft e mail box would this amount to an interception?   * **Issues**   *Is the message being transmitted?*   * **Points for discussion**   Most states require the police to establish a high threshold of suspicion before authorising the interception of the contents of a communication. Obtaining evidence without the requisite authority may result in the case being stopped or the evidence being inadmissible.  Computers and the internet facilitate a number of different forms of communication, e.g. e mail, instant messaging, twitter, etc. Messages will frequently be stored before they are retrieved by the intended recipient. Is a message that has yet to be retried still to be regarded as being in the course of its transmission? There is no way of knowing whether the draft message has been read by the intended recipient. Should the law grant the same protection to those who deliberately choose to subvert the normal means of sending communications by e mail as it gives to those who use e mail as it was designed to be used?  This is a fairly common way for criminals to communicate with each other. Whether seeking to access such messages in an interception or not will depend on domestic legislation and or the attitude of the domestic courts but it may be worth delegates realising that if they need to rely on Mutual Legal Assistance to obtain such data the requested state may consider it an intercept or at the least because access to the contents of a communication are being sought will have a higher legal threshold that needs to be established in order to obtain the necessary judicial authority . |
| **Case Study 4**   * **Fact/ scenario**   Police Officer Bobby has taken his wife’s phone, guessed her password and listened to a stored voice message that she has not yet retrieved.  *Is this an interception?*   * **Issues**   *Is the voice message still in the course of its transmission? Has there been an interception of computer data?*   * **Points for discussion**   Until the message has reached its destination it is probably still in the course of being transmitted even though it is stored within the system. The message is probably being digitally stored on the phone companies’ server and thus Bobby has accessed computer data. Is a phone a computer? Probably yes, it undertakes the automated processing of data. Police officers conducting searches who find phones may need to consider this in order to ensure that they have the necessary authority to access such messages. It would be different if the recipient had listened to the message and opted to store it.  This scenario raised similar issues to the previous scenario. It serves to illustrate what might be a fairly common situation that can equally apply to officers who executing a search warrant seize a computer which contains both opened and unopened e mail. It also serves to illustrate that the offence established under Article 3 applies to all forms of electronic data transfer, whether by telephone, fax, e-mail or file transfer. |
| **Case Study 5**   * **Facts/ scenario**   Bobby is interested in UFOs and he believes that the Russian Government has captured an alien space craft that landed in Siberia in the early part of the 20th Century. He visits a Russian Military recruitment site which has a link to a site operated by the Russian Air force. The Air Force site requires a password but using a password cracking tool he manages to gain access. He spends some time exploring the system and copies a number of files. He also tries to delete all of the log files of his activity in order to prevent the Russians from identifying him. He then alters the front page of the site so that it displays a picture of a UFO instead of the Air Force insignia .  *Has Bobby committed an offence?* Issues *Can unauthorised access of itself amount to an offence of Data or System Interference?*  *Does erasing the evidence of unauthorised access amount to an offence?*  *Does serious harm have to be caused to the operation of the computer before criminal liability is incurred?* Points for discussion The aim of these provisions is to provide computer data and computer programs with protection similar to that enjoyed by corporeal property against intentional infliction of damage.  Bobby was not authorised to access the Air Force site, it was password protected. Access therefore would constitute an offence of illegal access.  Bobby has deleted data , the log files and the Air Force insignia.Though perhaps he generated the log files they are not his, the system was configured to record such activity. He has no right to delete them. The Air Force may wish to know who has access to their system.  By altering the image on the front page he has both deleted and added data to the system which, whilst it is unlikely to have resulted in any important information having been lost, would be an embarrassment to the Air force. However, more importantly though Bobby may claim that he only accessed the system to find information and that he only deleted logs or other data of no importance can any systems administrator have confidence in the integrity of the data following such an unlawful intrusion?  Whether an offence has been committed in these circumstances will be a matter of local interpretation. It may be that the seriousness threshold has not been established. However the systems administrator would probably feel obliged to take the site off line in order in order to establish the effect of the intrusion, particularly if the site that has been accessed contains confidential or sensitive data or is used in operations which, if they were to go wrong would endanger the public such as a system responsible for running a nuclear power station.  If for the sake of argument the system that Bobby accessed was that used to run a nuclear PowerStation would the offences set out in Articles 4 and 5 be adequate to reflect the seriousness of such an intrusion which amounts to an attack on the National Critical Infrastructure? |
| **6. Case Study 6** Facts/ scenario An automated spam e mail programme sends unsolicited e mails to thousands of users all around the world every day. If the e mail is opened it downloads software to the user’s machine. The software does nothing which affects the running of the users computer, it doesn’t acquire data from the users computer nor does it delete any data or cause any other sort of damage, however it means that the users computer is now a ‘Zombie’ forming part of a ‘Botnet’ which the ‘bot controller’ can use to undertake various types of activity.  *Has an offence contrary to Article 4 or 5 been committed by the person responsible for sending the spam?*   * **Issues**   *Has there been any unauthorised access to the users machine? Has data been altered on the users machine ?*  *Has there been any damage to the users machine?*   * **Points for discussion**   Even though no damage has been caused the software brings about an alteration of the data on the users computer. That alteration was not authorised as the user was not given any warning or asked to consent in any way to the modification of his computer. Is the sending of Spam itself illegal or is it merely a nuisance? Does it only become illegal when it has an adverse impact?  What if the spam e-mail contained an attachment and invitation to the recipient to open the attachment saying “you will like this” ?  It might be argued that the recipient has chosen and thereby consented to downloading data to his computer. The reality however is that any consent that may have been given has not been an informed consent though it may be argued that those who choose to open attachments from unknown recipients do so at their own risk.  Does it make any difference that the user doesn’t care whether their computer became part of ‘bot net’ or not?  As we travel around the internet we visit sites and download data without giving proper consideration to the nature of the material that may be finding its way onto our computer but trusting to the names that websites give themselves, the names of files or the results returned by our search engine to make our decisions. Clicking on a thumbnail image of a picture in order to acquire a full size image indicates an awareness of the data that we are seeking to acquire and a fully informed consent as to the nature of that data. Should we click on a thumbnail image of a motor car only to find that the full size image we have acquired is that of an aeroplane we cannot be said to have given our consent to the acquisition of that data.  Choosing to open a link to a website will result in a lot of data being downloaded. If the site is a legitimate one the bulk of that data will probably relate to the content of the website though a proportion may consist of advertisements placed by third parties. Again we have made an informed choice and given an implicit consent to receive the advertisement knowing that this is a common practice on the internet. A common practice in the internet industry is to download data to the users internet browser , ‘cookies’.  Cookies perform a variety of functions including recording a users web browsing history. A user will be given the option to disable the cookie function on the browser, is such an option sufficient to imply that the user has subsequently given their consent to the downloading of such data? |
| **7. Case Study 7**   * **Facts / scenario**   Bobby is a former police officer who was sacked for improper use of the police computer system. He decides to get his own back on the police department. He uses an e mail programme which enables him to send 70,000 e mails per hour to his old department. He alters the e mail header to make it appear that it came from the chief officer of police thus fooling the police e mail server into believing that it came from a legitimate source. The police server was unable to handle the volume of traffic and collapsed.  *Is this an offence of system interference?*   * **Issues**   *Sending an e mail involves accessing or seeking to access a computer system, the e mail* server. *To what extent does the owner of such a server authorise such access?*  *If you have an e mail address does that not mean that you are inviting others to send you e mail messages?*   * **Points for discussion**   The question is one of right. Bobby has accessed a system and caused the system to collapse by inputting data. By establishing an e mail address which is accessible to the public the owner of the address is implicitly giving their consent to the receipt of messages. Bobby might argue that the police have consented to the receipt of each individual e mail and that is not his fault that their system lacked the capability to handle so many messages. But has their really been consent? The owner of a house grants an implied consent for the postman to post letters through his letter box that are addressed to the owner. There is also an implied consent to receive ‘junk’ mail such as pizza flyers. The homeowner however does not consent to receiving so many pizza flyers that he is unable to open his front door.  Might it not also be said that by altering the details of the sender of the e mail access to the e mail server has been gained through fraud? Consent is not given to the receipt of such ‘spoofed’ e mails.  Whilst this scenario concerns e mails the principle is good for those who seek to cause websites to collapse through a denial of service attack whereby the site is unable to handle the volume of traffic directed towards it. Connecting to a website involves the exchange of data between the users computer and the website. Similar issues as to implied consent to connect to the site arise as discussed in relation to email messages. |
| **Case Study 8**   * **Facts/ scenario**   Bobby sends an e mail to his estranged wife at her place of work. He alters the header to make it appear that it has come from one of her friends. The e mail contains a programme called ‘access all areas’ which allows Bobby to assume control over his wife’s computer. Before Bobby has the chance to use the programme its presence is detected by the system administrator who shuts down the system in order to undertake an evaluation of the extent of the intrusion.  *Has Bobby committed an offence contrary to Article 5?*   * **Issues**   Has Bobby brought about a suppression of data held on the system? Has Bobby hindered the functioning of a computer system?  Has any such suppression of data or hindrance to the functioning of the system been without right?   * **Points for discussion**   The response of the system administrator to Bobby’s e mail means that service has been denied to the users of the system. Access to data held on the system has therefore been suppressed, albeit it the restriction on access is likely to be temporary. The offence does not require data to be permanently unavailable.  We have discussed the extent to which the owner of an e mail address grants  consent to the receipt of data from others.  Article 5 concerns computer systems, that is one or more computers linked together. Is a lone computer connected to the internet part of a system?  Bobby’s wife’s work computer is more likely than not part of a system , she is probably part of a LAN ( Local Area Network) or WAN ( Wide Area Network) or Intranet . Has Bobby hindered the working of the system?  Bobby might argue that he is not responsible for the denial of service and that he had no intention to bring about such an event, in fact quite the opposite he wanted the system to carry on running so that he could find out what his wife was up to. Frequently denial of service attacks are insufficient to take a website off line , however service providers will take the site offline in order to minimise the effect of the attack on its systems and minimise inconvenience to other customers.  In this scenario Bobby does not appear to have the requisite intention for an Article 5 offence though this does not mean of course that he escapes criminal liability.  This is an example of a Trojan virus which is a common way for cyber criminals to gain access to the computers of others. |
| **9. Case Study 9**   * **Facts/ scenario**   An online internet ”hacktivist” group who are protesting against the use of animals to test cosmetics undertake ”Distributed Denial of Service” (DDOS) attacks against the websites of cosmetic companies , and glamour magazines. Through their website the group distribute software they call the ‘Supergun’ which enables the group to co ordinate attacks on websites and to thereby maximise the amount of traffic seeking to access a website at a particular time. The ‘Supergun’ software was originally developed as a tool by systems administrators to test the security of their systems. However whilst the software still works in exactly the same way the user interface has been rendered much easier to use and now bears the logo of the group.  *Is it an offence to make the Supergun available for downloading? Is it an offence to be in possession of the Supergun?*   * **Issues**   Does the fact that the Supergun can be used for a legitimate purpose mean that a prosecution cannot be brought?  Does making the Supergun available to be downloaded amount to distribution?   * **Points for discussion**   The offences to which this Article relates are; unauthorised access, illegal interception, data and system interference.  Whilst the software was originally dual use, that is had a legitimate function, now that the user interface has been modified does this mean that its possession etc is an offence?  Looking back at our previous case studies, the ‘access all areas’ software used by Bobby to gain access to his wife’s computer has a legitimate use. Programmes such as this allow users to access their own computers remotely What about Bobby’s possession of password cracking software; would this be an offence? May be an issue of intent, what legitimate reason does he have to possess such software? Is there any evidence to show that he has sought to deploy this software in order to commit an offence?  This offence is not designed to be used to criminalise legitimate software providers and users. Where, as there is here, evidence of a malicious intent the problem does not perhaps arise. However those involved in cybercrime are also frequently involved in legitimate internet activity and may well be industry professionals who use and develop such software but whom , when opportunity presents itself are prepared to deploy it in furtherance of illegal activity . What about shopkeepers? how are they supposed to know what intention a customer might have in relation to a particular piece of hard ware or software. Is the ambit of the offence too vague? |
| **Case Study 10**   * **Facts/ scenario**   A software provider has produced encryption software. The software divides the contents of the hard drive into two volumes, each requires a password to access however only one volume is visible to the ordinary user and the existence of the hidden volume cannot be detected using forensic software that is currently available.  The manufacture claims that this software would be of use to anyone who may find themselves in a situation where they are under coercion to reveal their password. It would mean that the data on the hidden volume can be kept secure even if they disclose the password to the visible folder.   * **Issues**   Does the manufacture, production, distribution use or possession of such software constitute a criminal offence?   * **Points for discussion**   We are all being constantly urged to keep our data secure. Whilst such a programme is obviously useful to those engaged in crime and in particular those who are fearful that the contents of their computers might incriminate them, the programme is not being used by them to commit an offence rather it is being used to conceal evidence.  Cyber criminals may make use of other programmes or systems to avoid detection including anonymizers which enable them to surf the internet without disclosing their true IP address or evidence eliminator programmes which can erase the contents of a hard drive. |
| **Case Study 11**   * **Facts / scenario 3**   Nick works for in the IT department of a large company which has its own intranet. Company policy forbids its employees from using their companies’ computer and internet connection to make online purchases. In his spare time Nick begins to develop software which would enable the company to identify those employees who are making online payments and to capture that information so that it can be used in evidence in disciplinary proceedings. Nick lacks the necessary skills and makes online contact with ‘Jupiter’. Together they develop a piece of software that once downloaded to a users computer will activate when that user begins to complete an online, form such as that used to process online payments and will capture the data inputted by the user. Nick’s company is very pleased whilst Jupiter begins to deploy the software using a Trojan programme.  *Has Nick committed an offence?*  *Has the company committed an offence? Has Jupiter committed an offence?*   * **Issues**   Has the device been designed or adapted primarily for the purposes of committing designated criminal offences?   * **Points for discussion**   Cybercriminals are able to access a variety of tools that enable them to commit offences or which will assist them in doing so. It is possible to purchase the code which will enable you to build your own ‘bot’ or purchase a ‘bot net ‘ or to purchase access to a bot net which will enable the user to undertake various types of crime such as ‘phishing’ .  Jupiter will use this programme to obtain financial information from users which can be exploited by either Jupiter himself or others. The company presumably thought that Nick had produced this during the course of his employment. Nick is innocent and has inadvertently helped Jupiter create a powerful criminal tool. Neither Nick nor the Company have the requisite criminal intent. Would it be different if Jupiter went on to market the programme to other companies who wished to monitor their employees internet activity? Could Jupiter argue that the software has a legitimate purpose despite its obvious attraction for criminals? |
| **Case Study 12**   * **Fact / Scenario**   Stefan uses a commercially available photographic software to produce a realistic bankers draft on his home computer. He takes the draft to his bank who accept it as genuine and transfer funds to Stefan’s account.  *What offence has Stefan committed?*   * **Issues**   Is the production of the forged bankers draft a computer related forgery?  Is the offence only completed once the bank clerk accepts the draft as being genuine?   * **Points for discussion**   Creating the bank draft involves inputting inauthentic data into a computer,  i.e. that the draft has been made out in favour of Stefan. However has this been done without right or has Stefan the right to produce such a document on his own computer? Stefan may have the intention to use the draft to defraud the bank but, for whatever reason may never get around to printing the draft. Does it make a difference to Stefan’s liability whether the document is ever produced on paper?  This offence was not really created to deal with this type of scenario though it may serve if domestic legislation would not otherwise criminalise the production of a forged banker’s draft These offences may better be considered in terms of secondary liability such as attempt.  This offence is really aimed at those who use a computer as the mechanism to commit the offence, thus when acting in good faith the bank clerk inputs the data supplied by Stefan accepting that the data is authentic. |
| **Case Study 13**   * **Facts/ scenario**   Stefan has always boasted to his friends of his prowess as an athlete when in his teens. His friends are sceptical. He manages to gain access to the database of his old school and alters the records to show him as captain of the school athletics squad and him having won a number of medals.  *Is this an offence of computer related forgery?*   * **Issue**   The data that has been altered will not be acted upon for any legal purpose.   * **Points for discussion**   Stefan has altered data and inputted inauthentic data. It is clear that this access and alteration is without right. Leaving aside the other offences that Stefan may have committed it is doubtful that he has committed a computer related forgery as this data will not be acted upon for legal purposes.  The forgery related offence is not concerned with financial or other gain; those offences come within the ambit of computer related fraud. This Article seeks to ensure the security and reliability of electronic data which may have consequences for legal relations. The term "for legal purposes" refers to transactions and documents which are legally relevant. |
| **Case Study 14**   * **Facts / scenario**   Now that he has lost his job in the Police Force and is having to pay alimony to his wife since their divorce Bobby is looking for another way to make money. He has always had an interest in share dealing and purchases 1000 shares in Flanders Mining Inc a company with an exclusive right to mine uranium in Belgium for 1 euro apiece. Bobby is a member of an internet forum whose members are, like Bobby, interested in the stock market. Bobby posts a message saying that a friend in the Belgium government has told him that substantial amounts of uranium have been detected in Belgium. Following this announcement the share price in Flanders Mining takes off, by the end of the week each share is worth 1000 euro. Bobby then sells his shares.  *Has Bobby committed an offence?*   * **Issues**   Is Bobbie’s message untrue?  If the message was untrue has another person lost property as a result? Has Bobbie gained an economic advantage?   * **Points for discussion**   If the message posted by Bobby is untrue then he may have committed an offence. He has inputted false data into a computer and has gained an economic benefit for himself in the rise in the share price.  Is the causal connection between the inputting of the data and the effect to remote?  Has Bobby caused a loss to another? Arguably yes in that the shares are incorrectly valued and will at some point presumably fall. However it has to be recognised that the market for shares is extremely volatile, is not the value of a  share the price that anyone is willing to pay for it at any particular time? Has anyone really been defrauded, are these types of rumours and messages not rife on the internet? is anyone really going to believe this post or fail to see it as a clumsy attempt to manipulate the share price ? Does this mean that we cannot tell lies on the internet? |
| **Case Study 15**   * **Facts/ scenario**   Stefan drives to the bank. In the car park he finds that he is short of change. He puts a washer into the automated parking machine and obtains a ticket.  *Has Stefan committed an offence?*   * **Issues**   Is the parking machine a computer?  Does it matter that the parking machine produces tickets automatically and no human being has been deceived?  What is the status of the parking ticket?   * **Points for discussion**   The parking machine is a computer, it processes data calculating the amount of money tendered against the parking tariff and issuing a ticket for the appropriate length of time. Stefan has inputted inauthentic data, the washer rather than the appropriate coin. Article 7 does not require a human to have acted on the data supplied.  The parking ticket is a forgery, the data used to create it was false and it was produced in order that a person, the car park attendant, would regard it as genuine and not give Stefan a parking ticket. |
| **Case Study 16**   * **Facts / Scenario**   After his arrest the police discover that Stefan is in possession of the credit card details belonging to a large number of third parties.  *Is the possession of this data a criminal offence?*   * **Issues**   What status do computer files have? Are they ‘things’ in law despite the fact that all they consist of is a string of binary code?   * **Points for discussion**   In the UK it is a substantive criminal offence to be in possession of an article for use in fraud. Article includes a computer file. Of course it is necessary to prove the necessary intent but it is difficult to argue a legitimate reason to have possession of data of this type.  It may be that this might be regarded as a preparatory offence. |
| **Case Study 17**   * **Facts/ scenario**   Adam is a member of an exclusive online group who exchange photographs of children being sexually abused. Adam is also a member of a ‘peer to peer’ file sharing group, he places photographs of children being abused that he has obtained from the online group into this peer to peer shared folders which makes it accessible to others on the peer to peer network.  *What offences has Adam committed?*   * **Issues**   Definitions of production, procurement and distribution.  Adam has downloaded image files from the internet. Does downloading equate to the production of such an image? Downloading, and particularly saving an image on a computer is not like watching TV. The act of downloading creates a new thing , a computer file thus viewing images on the internet involves the making of new images. Prosecutors may find this concept useful.  Peer to Peer file sharing networks allow members to access files made available to them by other members of the network . By placing the images into the shared folder Adam is making them available for distribution. |
| **Case Study 18**   * **Facts / scenario**   Bill is arrested at the airport on his return from Cambodia . His laptop is found to contain a large number of images of him engaged in sexual activity with children who appear to be from South East Asian.  *Can Bill be prosecuted in respect of the images?*   * **Issues**   Jurisdiction.  Choice of substantive offence, being in possession of an image or making the image.   * **Points for discussion**   There may be jurisdictional issues in relation the making of the images as these appear to have been produced overseas.  Possession should not be a problem. |
| **Case Study 19**   * **Facts / scenario**   [WWW.Iuvfishin.com](http://WWW.Iuvfishin.com/) is a Website devoted to fishing. The site is hosted on servers located in the USA The owners of the site discover that it had been hacked and that a thousand child abuse images have been uploaded and embedded within the site. The way it has been done means that these images would not be visible to ordinary users of the site. The site logs the IP addresses of those who have accessed the photographs.  An IP address attributed to John has been given to the police in your country They search John’s address and seize his computer which contains thousands of child abuse images. It is clear from the internet history and the data within these files that most of the images have been downloaded from the internet.   * **Issues**   How to prove that John is responsible for the images? The impact on suspects accused of paedophile offences**.**   * **Points for discussion**   This method of concealing images is not uncommon. Groups will post links to the images. However, it may be dangerous to rely on the IP address alone to obtain a search warrant without understanding how that IP address came to be logged on the site , they could have got their entirely innocently having been referred by another site and not gone on to access any images once they realised what they were . Of course they may have visited on more than one occasion or accessed a number of images.  Can use this to discuss the care needed before accusing ain individual of being a paedophile. There is a high rate of suicide amongst persons accused of these offences. As in all cyber crime cases you need to be able to put the suspect at the keyboard at the relevant time , an IP address may be used by a number of individuals at the same address or the wireless network may have been hijacked by someone else. Accusations of this type can have a devastating effect on an innocent individual. |
| **Case Study 20**   * **Facts / scenario**   The police in the USA have taken down a website that hosts sites offering child abuse images for those who pay a monthly subscription. The USA authorities have captured data from those who have paid for access, including IP address, credit card numbers, e mail address, billing address and password. One of the customers is Oswald. Having obtained a search warrant his computer is examined. Nothing incriminating is found because Oswald has used a programme called “Elimination of Evidence”  *Has Oswald committed an offence?*   * **Issues**   Has Oswald committed a substantive offence or one of secondary liability? Are there issues about jurisdiction?  Does it matter that the US website was fully automated?  What do we say about the use of the Evidence Elimination programme?   * **Points for discussion**   Oswald is not in possession of any images and we cannot prove that he ever accessed a website to view such images albeit that we can prove that he paid a subscription in order to do so. However Oswald has paid money in order to persuade another person, the website owner in the USA to distribute or make available child abuse images for distribution. Does this therefore constitute an offence?  That the US website if fully automated means that no human being is actually involved in the processing of the credit card details. Even so, the process was created by and is administered and maintained by a person who is profiting financially.  The use of an evidence elimination programme is not, per se illegal. Unless Oswald was able to activate the programme during the course of the police investigation he is unlikely to have committed an offence connected with the  administration of justice. However if Oswald is prosecuted the use of such programmes may be regarded as an aggravating feature by the court. |