I'm not a bot

Share — copy and redistribute the material in any medium or format for any purpose, even commercially. Adapt — remix, transform, and build upon the material for any purpose, even commercially. The licensor cannot revoke these freedoms as long as you follow the license terms. Attribution — You must give appropriate credit , provide a link to the license, and indicate if changes were made . You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use. ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original. No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits. You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable exception or limitation . No warranties are given. The license may not give you all of the permissions necessary for your intended use. For example, other rights such as publicity, privacy, or moral rights may limit how you use the material. It is against the law to access a computer without being authorisedIt is against the law to access a computer or data with the intent to commit a crime or perform illegal activityIt is against the law to modify data without permission. Previous WIMP This guidance sets out how to consider prosecuting cases under the Computer Misuse Act 1990 (‘CMA’). It also provides guidance on offences relating to the collection, processing, and storage of personal data under the Data Protection Act 2018 (‘DPA’). For a general overview on cybercrime, please see the Legal Guidance on Cybercrime.DefinitionsThe CMA does not provide a definition of a computer because rapid changes in technology would mean any definition would soon become out of date.Definition is therefore left to the Courts, who are expected to adopt the contemporary meaning of the word. In DPP v McKeown, DPP v Jones ([1997] 2 Cr. App. R. 155, HL, at page 163), Lord Hoffman defined a computer as "a device for storing, processing and retrieving information." The Council of Europe Cybercrime Convention 2001 ('Budapest Convention') definitions may also assist:"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."Computer data": 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 DPA defines personal data as any information relating to an identified or identifiable living individual.JurisdictionUnder section 4 CMA, liability for offences under sections 1, 3 or 3ZA requires proof of at least one ‘significant link’ with the ‘home country’ concerned (i.e. England and Wales)'. A significant link could include:The accused is in the home country at the time of the offenceThe target of the CMA offence is in the home countryThe technological activity which has facilitated the offending may have passed through a server based in the home countryAs defined in section 5, in relation to an offence under Section 3ZA, any of the following is also a significant link with domestic jurisdiction:That the accused was in the home country concerned at the time when s/he committed the unauthorised act (or caused it to be done);That the unauthorised act was done in relation to a computer in the home country concerned;That the unauthorised act caused, or created a significant risk of, serious damage of a material kind (within the meaning of that section) in the home country concerned.As defined in section 6, the extended extra-territorial jurisdiction arrangements also apply to conspiracy or attempts to commit offences under the CMA and therefore will supersede the usual rule for conspiracy chargesThe OffencesSection 1: Unauthorised access to computer materialThe maximum penalty on indictment is 2 years imprisonment. Sections 1 and 2 of the CMA must be read in conjunction with the interpretation section at Section 17.Actus ReusThe offence is made out once a defendant has caused a computer, which would include his own computer, to perform a function with intent to secure access.This excludes mere physical contact with a computer and the scrutiny of data without any interaction with a computer (thus the reading of confidential computer output, the reading of data displayed on the screen, or 'computer eavesdropping', are not covered).The access to the program or data which the accused intends to secure must be 'unauthorised' access.Mens reaThere are two elements:There must be knowledge that the intended access was unauthorised; andThere must have been an intention to secure access to any program or data held in a computer.The word 'any' makes it clear that the intent need not relate to the computer which the accused is at that time operating. Section 1(2) explains that the intent of the accused need not be directed at any particular program or data, so as to include the hacker who accesses a computer without any clear idea of what he will find there.There has to be knowledge on the part of the offender that the access is unauthorised; mere recklessness is not sufficient. This covers not only hackers but also employees who deliberately exceed their authority and access parts of a system officially denied to them.In the case of R v Bow Street Magistrates' Court and Allison (AP) Ex Parte Government of the United States of America (Allison) [2002] 2 AC 216, the House of Lords considered whether an employee, who was authorised to access certain client accounts, could commit an offence securing 'unauthorised access'. It was held that the employee clearly came within the provisions of Section 1, as she intentionally caused a computer to give her access to data she knew she was not authorised to access (which she then passed on to others who were able to forge credit cards). The House of Lords made it clear that an employee would only be guilty of an offence if the employer clearly defined the limits of the employee's authority to access a program or data.This judgment contrasts with the earlier case of DPP v Bignell [1998] 1 Cr App R8, where two police officers, who were authorised to request information from the police national computer (PNC) for policing purposes only, requested a police computer operator to obtain information from the PNC which, unbeknown to the operator, was for their own personal use. The Divisional Court held that the two officers had not committed a Section 1 unauthorised access offence. The House of Lords, in Allison confirmed the conclusion of the Divisional Court in the earlier case. The House of Lord's went on to say that:"it was a possible view of the facts that the role of the officers in Bignell had merely been to request another to obtain information by using the computer. The computer operator did not exceed his authority. His authority permitted him to access the data on the computer for the purpose of responding to requests made to him in proper form by police officers. No offence had been committed under section 1 of the CMA." When dealing with cases involving employees careful consideration should be given to the employee's contract of employment, together with any surrounding information (for example oral advice given or office practices amongst others), in order to determine whether the employer had clearly defined the limits of the employee's authority. Such cases normally depend on whether the evidence available demonstrates sufficiently that the conduct complained of was unauthorised.In certain circumstances consideration should be given to the Data Protection Act 2018. (See Alternative Offences below).Section 2: Unauthorised access with intent to commit or facilitate commission of further offencesThe maximum penalty on indictment is 5 years imprisonment.The offence under Section 2 is committing the unauthorised access offence under Section 1 with intent to commit or facilitate the commission of a more serious 'further' offence. It is not necessary to prove that the intended further offence has actually been committed.Examples of such offences are obtaining the unauthorised access with the intention of committing theft, such as by diverting funds, which are in the course of an electronic funds transfer, to the defendants own bank account, or to the bank account of an accomplice; or where the defendant gained unauthorised access to sensitive information held on computer with a view to blackmailing the person to whom that information related.A person found not guilty of a section 2 or 3 offence by a jury can be convicted of a section 1 offence see Criminal Law Act 1967 section 6(3). Section 3: Unauthorised Acts with intent to impair, or with recklessness as to impairing the operation of a computerThe maximum sentence on indictment is 10 years' imprisonment.The effect of Section 3 is that a person commits an offence if he performs any unauthorised act in relation to a computer, knowing it to be unauthorised, if he intends by doing the act to do one of the things set out in Section 3(2), or if he is reckless as to whether by doing the act he will do one of the things set out in Section 3(2).Examples of this are deliberate or reckless impairment of a computer's operation, preventing or hindering access to computer material by a legitimate user or impairing the operation or reliability of computer-held material. The offender must know that the act was unauthorised. In DPP v Lennon (2006) 170 JP 532, Section 3 should be considered in cases involving distributed denial of service attacks (DDoS), as the term "act" includes a series of acts, there is no need for any modification to have occurred and the impairment can be temporary.DDoS is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet using incoming traffic originating from many different sources flooding the victim, making it difficult to stop the attack by blocking just one source. It has been compared to crowds of people blocking an entrance to business premises making it impossible for legitimate customers to enter and thereby disrupting trade.If a computer is caused to record information which shows that it came from one person, when it in fact came from someone else, that manifestly affects its reliability and thus the reliability of the data in the computer is impaired within the meaning of Section 3(2)(c): Zezev and Yarimaka v. Governor of H.M. Prison Brixton [2002] EWHC 589 (Admin).Simply modifying the contents of a computer is not criminal damage within the meaning of Section 10 of the Criminal Damage Act 1971. In Cox v Riley (QBD) 1986, the court stated that it shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.Section 3ZA: Unauthorised acts causing, or creating risk of, serious damageSection 41(2) of the Serious Crime Act 2015 inserted section 3ZA, with effect from 3 May 2015.The maximum sentence on indictment is 14 years, unless the offence caused or created a significant risk of serious damage to human welfare or national security, as defined in Section 3 (a) and (b), in which case a person guilty of the offence is liable to imprisonment for life.Section 3ZA is designed to cater for computer misuse, where the impact is to cause damage to, for example, critical national infrastructure and where the maximum penalty of ten years available under Section 3 may be inadequate.When considering, the definition of “critical national infrastructure”, (in line with European Directive (2013/40/EU)) it could be understood to be an asset, system or part thereof located in Member States, which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, such as power plants, transport networks or government networks, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.Particular consideration should be given to the required mens rea and actus rea for this offence.Cases in which a section 3ZA charge is being considered, given the nature of such cases, should be referred to SEOCID. Section 3A: Making, supplying or obtaining articles for use in offence under Section 1, 3 or 3ZAThe maximum sentence on indictment is two years' imprisonment.The rationale behind the creation of this offence is the market in electronic malware or 'hacker tools'; which can be used for breaking into, or compromising, computer systems.Whilst there is no definition of ‘article’ in CMA, section 8 of the Fraud Act 2007 states that an ‘article’ includes any program or data held in electronic form.The prosecution has to prove the defendant had the necessary intent. Possession alone is not an offence.Section 3A(2) of the CMA covers the supplying or offering to supply an article 'likely' to be used to commit, or assist in the commission of an offence, contrary to Sections 1 or 3. 'Likely' is not defined in the CMA but, in construing what is 'likely', prosecutors should look at the functionality of the article and at what, if any, thought the suspect gave to who would use it. For example, whether the article was circulated to a closed and vetted list of IT security professionals or was posted openly. In the offence under Section 3A(2), the relevant mens rea is 'belief' and mere suspicion is not enough. In determining the likelihood of an article being used (or misused) to commit a criminal offence, prosecutors should consider the following:Has the article been developed primarily, deliberately and for the sole purpose of committing a CMA offence (i.e. unauthorised access to computer material)?Is the article available on a wide scale commercial basis and sold through legitimate channels?Is the article widely used for legitimate purposes?Does it have a substantial installation base?What was the context in which the article was used to commit the offence compared with its original intended purpose?Public InterestWhere there is sufficient evidence to meet the evidential test under the Code for Crown Prosecutors, the following Public Interest factors should be carefully considered:The financial, reputational, or commercial damage caused to the victim(s);The offence was committed with the main purpose of financial gain;The level of sophistication used, particularly sophistication used to conceal or disguise identity (including masquerading as another identity to divert suspicion);The victim of the offence was vulnerable and has been put in considerable fear or suffered personal attack, damage or disturbance;The mental health, maturity and chronological age of the defendant at the time of the offence.CMA suspects can be disproportionately represented by individuals who are under 18 and may be more neurologically diverse than other types of offenders. Further guidance can be found on these matters can be found in the legal guidance on Youth Offenders and Suspects with Mental Health Conditions.Alternative OffencesWhen considering charging for CMA offences, in line with paragraph 2.5 of the Code for Crown Prosecutors, consideration should be given as to whether the most appropriate offence is being prosecuted. CMA offences are often committed as a precursor to another offence such as fraud or blackmail. In these circumstances a prosecutor may decide to charge the offence for which the sentence is likely to be higher in order to reflect the nature of the offending.Fraud Act 2006Prosecutors may wish to consider whether the 'article' might be intended for use in fraud and consider whether there is an offence contrary to Section 7 and/or Section 6 of the Fraud Act 2006. For example phishing (false financial e-mails), pharming (cloned false websites for fraud) and Trojan installation (viruses) could be prosecuted under the Fraud Act.An offence of making or supplying articles for use in fraud, contrary to Section 7, is punishable by a maximum of 10 years' imprisonment. An offence of possession of articles for use in fraud contrary to section 6 is punishable by a maximum of 5 years' imprisonment.Investigatory Powers Act 2016Unlawful interception of a public telecommunication system, a private telecommunication system, or a public postal service,Misconduct in Public OfficeThe common-law offence of misconduct in public office, for example, where a police officer misuses the PNC.Data Protection Act 2018DPA 2018 creates a number of offences in relation to the control and access to data:Section 119: Creates offences relating to the obstruction of inspections of personal data by the Information CommissionerSection 132: Creates an offence for persons who are currently or have previously been the Information Commissioner, a member of the Information Commissioner's staff or an agent of the Information Commissioner from disclosing information obtained in the course of, or for the purposes of, the discharging of the Information Commissioners functions unless made with lawful authority.Section 144: Creates an offence for a person to intentionally or recklessly make a false statement in response to an information noticeSection 148: Creates an offence where the Information Commissioner has given an information notice or an assessment notice requiring access to information, a document, equipment or other material, it is an offence to destroy or otherwise dispose of, conceal, block or (where relevant) falsify it, with the intention of preventing the Commissioner from viewing or being provided with or directed to it.Section 170: Creates an offence of the deliberate or reckless obtaining, disclosing, procuring and retention of personal data without the consent of the data controller.Section 171: Creates a new offence of knowingly or recklessly re-identifying information that has been de-identified without the consent of the controller who de-identified the data. This responds to concerns about the security of de-identified data held in online files. For example, recommendations in the Review of Data Security, Consent and Opt-Outs by the National Data Guardian for Health and Care called for the Government to introduce stronger sanctions to protect de-identified patient data.Section 173: Creates an offence of the alteration of personal data to prevent disclosure following the exercise of a subject access right. The relevant subject access rights are set out in subsection (2).Section 184: Creates an offence for an employer to require employees or contractors, or for a person to require another person who provides goods, facilities or services, to provide certain records obtained via subject access requests as a condition of their employment or contract. It is also an offence for a provider of goods, facilities or services to the public to request such records from another as a condition for providing a service.In England and Wales, proceedings for an offence under this Act may be instituted only (a) by the Information Commissioner, or (b) by or with the consent of the Director of Public Prosecutions.Sentencing CasesThere are no official guidelines for sentencing for offences under CMA. The below are examples of precedent sentences.R v Mudd [2018] 1 Cr App R (S) 33 (7)The offender, who was aged between 16 and 18 over the course of the offending, admitted offences under sections 1 and 3, and a further offence of concealing criminal property. He had devised a distributed denial of service program which he used on some occasions himself and on other occasions supplied the program for payment for others to use. In total, 1.7 million DDoS attacks were carried out directed at well over half a million individual IP addresses or domain names. The defendant received in the order of 250,000 total payment for the DDoS program supplied.Psychological and psychiatric reports indicated the offender was autistic. Having reviewed these, the judge imposed a sentence of detention in a young offender institution for two years, given the scale of the offending. The Court of Appeal upheld the custodial sentence but reduced it to 21 months.R v Brown (Charles) [2014] EWCA 695Charles Brown, 39, was convicted of one count of possession of articles for use in fraud, contrary to section 6 (1) of the Fraud Act 2006 and two counts of securing unauthorised access to computer material with intent, contrary to section 2 (1) of the CMA. The CMA counts related to access to bank accounts. The basis of the fraud count was possession on the appellant's computer of the stolen bank and credit card details.The appellant's modus operandi involved changing details online and the subsequent impersonation of the account holders in order to obtain a new card and PIN.There was no actual loss - the potential loss from the 83 accessed accounts was almost £500,000 but that was based on the maximum credit limits for the accounts. The appellant and the prosecution agreed that the potential loss was in fact just over £200,000.The trial judge sentenced him to a total of three years' imprisonment.The Court of Appeal set aside the sentence, noting that while potential loss is an aggravating feature it is not the determining means by which the fraud should be valued and imposed a total of two years' imprisonment.R v Martin (Lewys Stephen) [2013] EWCA Crim 1420Lewys Martin, aged under 21 at the time of the offences, pleaded guilty to offences contrary to section 1, 2, 3 and 3A CMA relating to DOS attacks against the Oxford and Cambridge University websites, the Kent Police website and offences targeting two private individuals (including unauthorised use of a person's Paypal account). His sentence of two years was upheld on appeal, the court noting the prevalence of computer crime, the fact that organisations were compelled to spend substantial sums combating it and the potential impact on individuals meant that sentences for such offences should involve a real element of deterrence.R.v Crosskey (Gareth) [2012] EWCA Crim 1645; [2013] 1 Cr.App.R.(S.) 76Gareth Crosskey, aged 19, pleaded guilty to offences under ss.1 and .3, having accessed the Facebook account of the step-father and manager of an actress. He persuaded Facebook staff to provide the password to the account. He contacted magazines offering to reveal information about her and contacted her stepfather to say he had access to her private emails and invited discussion as to what would prevent him from doing further damage. Southwark Crown Court sentenced him to 6 and 12 months' custody, concurrent, for the sections1 and 3 offences, respectively.On appeal, the court referred to the "seriously aggravating features" of the offence, namely the element of harm to the actress and her step father. The court rejected the argument that the sentence should have been suspended. However, having regard to the mitigating factors, namely the appellant being a young man of previous good character, the offending taking place over a short period of time and the appellants' expression of remorse, the sentence was reduced to four and eight months, concurrent, in a young offender institution.R v Mangham (Glen Steven) [2012] EWCA Crim 973; [2013] 1 Cr. App. R. (S.) 11Glen Mangham, aged 26, pleaded guilty to three offences under sections 1 and 3, having accessed Facebook's computers and modified the functionality of various programs. It cost Facebook $200,000 to respond to the incident. Southwark Crown Court sentenced him to eight months' custody, concurrent, on each count and a Serious Crime Prevention Order was imposed. On appeal, the court identified a number of aggravating factors which would "bear on sentences in this type of case":whether the offence was planned and persistent;the nature of the damage caused to the system itself and to the wider public interest such as national security;individual privacy;public confidence;commercial confidentiality;the cost of remediation, although that was not a determining factor.Motive and benefit were also relevant, as was revenge. Other factors to be considered were any financial benefit from the sale of the accessed information, whether the information was passed on to others, and the value of the intellectual property involved.Among the mitigating factors the psychological profile of the offender deserved "close attention". The Court upheld the appeal, substituting a sentence of four months' imprisonment.Further AssistanceCyber Leads in the Serious Economic, Organised Crime and International Directorate are able to offer further assistance. It is against the law to access a computer without being authorisedIt is against the law to access a computer or data with the intent to commit a crime or perform illegal activityIt is against the law to modify data without permission. Previous WIMP 10. Savings11. Proceedings for offences under section 1.12. Conviction of an offence under section 1 in proceedings for an offence under section 2 or 3.13. Proceedings in Scotland.14. Search warrants for offences under section 1.15. Extradition where Schedule 1 to the Extradition Act 1989 applies.16.Application to Northern Ireland.16A.Northern Ireland: search warrants for offences under section 117. Interpretation.18. Citation, commencement etc. The main purpose of the Computer Misuse Act (CMA) was to tackle cyber crime by making unauthorised access to, and modification of, computer data illegal. The Act represented the first major legislative attempt to tackle cyber threats and criminalise hacking, viruses, malware, and spyware. Main Provisions of the Act The Computer Misuse Act applies to any digital operation with a significant link to the United Kingdom. This covers situations where a computer being targeted is in the UK; if the person responsible carried out the operation from the UK; if they used a server located in the UK; or if the resulting cyberattack caused damage within the country. Section 1 of the Act criminalises hacking and what it describes as ‘unauthorized access to computer material’. A person is guilty of an unauthorised act if they attempt to access information that they are aware they are unauthorised to access. Section 2 then addresses ‘unauthorized access with intent to commit, or facilitate commission of, further offenses’. This is when the hacker, already guilty under Section 1, has carried out the hacking because they intend to commit more crimes, such as extortion or fraud, using the data they have accessed. Section 3 of the Act then refers to unauthorized acts with the intent to impair the operation of a computer, either recklessly or intentionally. Again, this section relies on a crime under Section 1 having been established and adds further penalties if the hacking meant to damage (such as through a virus) or alter the computer or computer system and its contents (such as through modifying, deleting data or introducing malware and spyware), or simply had this effect as a result of the unauthorised access. All crimes under the Computer Misuse Act can result in a fine and potential imprisonment. Why was the 1990 Computer Misuse Act introduced? The Computer Misuse Act’s purpose was to regulate the growing world of computers, which back in 1990 was simply not adequately protected by law. The growth of computers during the 1980s led to the Computer Misuse Act of 1990. Concerns around the relevance of the existing legal framework to computers was brought to light with the 1987 case of Steve Gold and Robert Schifreen, who gained unauthorised access to a BT service, which eventually led to them accessing the Duke of Edinburgh’s email account. Their conviction under the Forgery and Counterfeiting Act 1981 was overturned on appeal, as the facts of the case did not match a criminal offence under existing legislation. The Computer Misuse Act still governs the wider digital environment, with the internet, smart phones, and social media emerging in the decades after the Act first gained Royal Assent. Subsequent Amendments to the Act In recent years there have been a number of amendments to the Computer Misuse Act. A 2006 addition to the original Computer Misuse Act, specifically outlawed the making, supplying or obtaining articles for use in an offense under Section. This now addressed the issue of people using malware, viruses and other such tools developed by others, for the purposes of hacking. Where the original 1990 Act had for the first time explicitly criminalised activities which damaged computers, in 2015, a further provision was added in relation to serious damage. This 2015 addition significantly increased the penalties for ‘unauthorized acts causing, or creating risk of, serious damage’. Under the 2015 change, ‘serious damage’ extended beyond the digital world and refered to damage to people, the environment, and States. The remit of the Act now expanded to cover the possibility of cyber-terrorism and a state backed cyber attack. Crimes which are committed, and which fall within the remit of ‘serious damage’, can now result in a maximum sentence of life imprisonment. Examples of the Act in action Over the years, a number of cyber criminals have been prosecuted under the Computer Misuse Act. For example, in a 2013 case, the Crown (R) vs Martin, 2013, saw a defendant, who had hacked several websites including those of the Universities of Oxford and Cambridge, pleading guilty to breaches of Sections 1, 2, 3 and 3A and receiving a sentence of two years’ imprisonment. In a 2014 case, the Crown (R) vs Brown, 2014, the offender, who was in possession of stolen bank details, was convicted of two crimes under Section 2 of the Act, as well as another count under the Fraud Act 2006, and sentenced to three years’ imprisonment, reduced to two on appeal. In a 2018 case involving a minor, the Crown (R) v Mudd, the accused confessed of crimes under Sections 1 and 3, as well as concealing criminal property, which is a crime outside of the Computer Misuse Act. The defendant was sentenced to two years in a young offenders’ institution, which was reduced to 21 months on appeal. In 2018, the Information Commissioner’s Office also prosecuted its first Computer Misuse Act case when a car accident repair firm employee repeatedly accessed personal data stored on a software system used by his firm with colleagues’ login details. The trial resulted in the defendant receiving a 6-month prison sentence. Calls for Reform of the Computer Misuse Act The Computer Misuse Act was designed to retain some flexibility in the face of a swiftly developing digital landscape. For this reason, ‘computer’ is undefined in the Act, allowing prosecutors to easily apply it to crimes involving new technology, such as smartphones. As discussed, the Computer Misuse Act has also been amended several times to uphold its relevance and effectivity in deterring cybercrime. According to an analysis of figures from HM Courts and Tribunals Service in 2019 by tech news website the Register, there were 441 prosecutions under the Computer Misuse Act between 2007 and 2018. In 2018, nearly 90% of these prosecutions resulted in convictions. However, out of the total of 45 convictions in 2018, only nine resulted in immediate prison sentences. In 2018, it was also equally likely for offenders under the Computer Misuse Act to receive an official caution rather than prosecution. Critics of the Act say that these figures show an attitude towards computer misuse that is too forgiving, and do not sufficiently deter people from breaking the law in this way, citing rising rates of cybercrime. Another concern with the Computer Misuse Act is that, since its introduction thirty years ago, an extensive cyber security research industry has developed. The Act is said to fail to sufficiently differentiate the activities of this cyber security industry from those of hackers seeking to commit crimes. Accordingly, so-called ‘white hat’ ethical hackers who test unauthorised access for research reasons, may be liable to prosecution under the current Act. Critics argue that this has worked to curtail the UK’s participation at the cutting edge of such research. Computer Misuse Act in Full The Computer Misuse Act can be read in full here. Back IntroductionThis law came in to being specifically to deal with hackers, people who seek to gain unauthorised access to computer systems. In the early days of computing, hackers were seen as 'a little bit naughty'. It soon became apparent that they could cause untold damage to national security, could cause havoc with a company's legitimate operations and could steal a lot of money from anyone, whose security is not perfect. This includes not just well-educated members of the public but OAPs and other vulnerable groups, who may not be completely confident with technology. This might be because they have not had the education to understand the latest technology or might be confused by it or trust hackers and scammers, who find ever-increasingly clever ways to gain people's trust. Existing legislation was difficult to apply to hackers. The result was the Computer Misuse Act 1990. The three principles of the Computer Misuse Act 1990 It makes it illegal to access data to which you have no right. For example, you are not allowed to try to guess or find out a friend's password and then gain access to their files - even if you don't change edit or delete them! You can be fined and jailed for up to 6 months. It makes a more serious offence of accessing data to which you have no right with the intention of carrying out other crimes. For example, if you hacked into a bank's system with the intention of stealing credit card numbers, then you would fall foul of this law. You can be fined and jailed for up to 5 years. It makes it illegal to change any data. If you hack into an area to which you have no right and start deleting files or modifying data then you will be breaking this law. You can be fined and jailed for up to 5 years. In addition, if you write, use or distribute a virus, worm or indeed any malware to attack a computer system, you are also committing an offence. This is known as Part 3a of the Computer Misuse Act 1990. In 2014, the Act was amended to increase the sentences for the most serious computer crimes under this Act. Some disadvantages of the Computer Misuse Act 1990There have been less than a handful of convictions using this Act and sentences are lenient in the UK compared to e.g. the USA. The Act therefore does little to deter people. It is difficult to track down people who commit the crimes for which the Act was written and difficult to prove intent. Companies who are attacked are sometimes less than enthusiastic about reporting crimes and pressing charges because they don't want to publicise how poor the security systems they had in place were. Back Computer Misuse Act Section 1: Unauthorised access to computer material. Actus Reus. Mens rea. Section 2: Unauthorised access with intent to commit or facilitate commission of further offences. Section 3: Unauthorised Acts with intent to impair, or with recklessness as to impairing the operation of a computer. What activities are illegal under the Computer Misuse Act? It is illegal to access data stored on a computer unless you have permission to do so. Unauthorised access is often referred to as hacking . It is illegal to access data on a computer when that material will be used to commit further illegal activity, such as fraud or blackmail. Is the Computer Misuse Act outdated? The Computer Misuse Act 1990 is now 30 years old and must be updated, according to the Criminal Law Reform Now Network (CLRNN), a group of academics from Birmingham and Cambridge universities that specializes in legal reform projects. Who broke the Computer Misuse Act? This constituted a breach of the CMA, with Doyle pleading guilty to conspiracy to secure unauthorised access to computer data, and selling unlawfully obtained personal data. Both Doyle and Shaw, as a result, have each been handed an eight-month prison sentence, suspended for two years. What are the four Offences of the Computer Misuse Act? These four clauses cover a range of offences including hacking , computer fraud, blackmail and viruses. Failure to comply with the Computer Misuse Act can lead to fines and potentially imprisonment. Is it illegal to send someone a virus? In the U.S. and most jurisdictions around the world, it is illegal to send viruses and malware. U.S. law is quite clear on this, as established by the Computer Fraud and Abuse Act of 1986. Is spreading a computer virus illegal? The US Patriot Act (sec 814) offers punishment for those who damage or gain unauthorized access to a protected computer, causing financial or medical damages. In most countries, it is NOT ILLEGAL to create a computer virus, but it is illegal to spread a computer virus. What does the Computer Misuse Act 1990 make it illegal to do? The Act also makes it an offence to make, adapt, supply or obtain articles for use in unlawfully gaining access to computer material or impairing the operation of a computer. Access is defined in the Act as: altering or erasing the computer programme or data. Has the Computer Misuse Act been updated? Introduced in 1990, the Computer Misuse Act is imposed against cybercriminals facing accusations such as hacking and data breaches. The Act has been consistently updated to address the ever-changing technology landscape and has been shaped to respond to a growing variety of threats. Is it illegal to send Trojans? Creating and distributing trojan horse computer software is illegal, as is managing a botnet and using computers for malicious purposes. Defendants who are involved with a trojan horse scam can be charged with very serious computer crimes, including violations of the federal Computer Fraud and Abuse act. Is it illegal to use a Trojan virus? Is it legal to send someone a virus? Is it illegal to give someone a computer virus? No. It is not against the law or a crime to make a computer virus, Trojan, or malware. However, if that virus spreads to other computers intentionally or by mistake, you’ve violated the law, and you could be held liable for any damages it causes. “The Computer Misuse Act means that computer users are criminalised for simply trying to learn how systems work”Discuss whether or not you agree with this statement. 9 marksHow to answer this question:Describe your knowledge of the Computer Misuse ActMention the three main offences Apply to a scenario, in this case the question hasn’t given us a full scenario so we can use our ownKeep the argument balanced, once you’ve spoken about one side, then speak about the otherThen write your conclusion and use your own opinionAnswer:Example answer that gets full marks:The Computer Misuse Act (CMA) is a provision for securing computer material against unauthorised access or modification to the system. Under the CMA there are three main offences that you can be prosecuted for; The unauthorised access to a computer system, the unauthorised access to the computer system with intent to make changes and unauthorised access to the computer system and making changes.Users can still investigate how computer systems work; they would just need to get authorisation before doing so. For example you could ask the owner of the computer system to allow access first or you could create a virtual computer system and use this to investigate. The CMA could however be broken by accessing an email account of somebody without permission. Ultimately users need to make sure that they are aware of the law when accessing any computer system. In conclusion I disagree with the statement “The Computer Misuse Act means that computer users are criminalised for simply trying to learn how systems work” as users are able to educate themselves on the details of the CMA easily online and therefore should know the consequences of accessing a computer system without the right authorisation. There are plenty of online platforms, programs and systems that are accessible to access virtually and would not be in breach of the CMA. Page 2The Data Protection Act (DPA) is a law that protects personal data from being misusedExamples of personal data would includeNameAddressDate of BirthRaceReligionMost people that store personal data has to follow the Data Protection Principles although there are a few exemptions:Domestic purposes – if you only use personal data for such things as writing to friends and family or taking pictures for your own enjoyment, you are not subject to the DPALaw enforcement – the Police investigating a crime is not subject to the DPA. E.g. if someone has been suspected of a crime they can't request to see the evidence about themIntelligence services processing – personal data processed by the intelligence services (eg MI5) is not covered by the DPAPrincipleHow does it affect a company?Example1. Personal data must be fairly and lawfully processedA company has to be clear about what personal data they wish to collect and what they want to use it for. A school can request personal data to be able to call guardians in an emergency.2. Personal data must be collected for specified and lawful purposesA company cannot use personal data for any purpose other than what they stated originally. They also cannot pass this data on without permission.A company asks for a phone number to call regarding delivery but then uses it to market new products. 3. Personal data must be adequate, relevant and not excessiveA company cannot request personal data that they do not need right away.A bank cannot ask for their customer's previous trips when opening an account.4. Personal data must be kept accurate and up to dateIf a company holds personal data that is wrong or out of date then you have a right to have it corrected or deleted. If a bank has a customer's old address then they will not be able to send up to date statements.5. Personal data will not be kept for longer than is necessaryA company must delete personal data once they no longer have a need for it. If a customer closes their account the company must delete their data. 6. Personal data must be processed in line with people's rightsIf requested a company must provide a customer with all the personal data they hold on them. A hospital has to give a patient’s full records if requested by the patient. 7. Personal data must be held securelyA company is required to make sure that personal data they keep is secured (usernames and passwords) and is backed up to prevent accidental loss. A company could make external backups on the cloud. 8. Personal data must not be transferred to countries outside the European Economic Area unless those countries have similar data protection lawsA company cannot send personal data outside the European Economic area unless the country in question has been deemed by the European Commission to provide a good level of protection of personal data. A company cannot send its data to China because they are not deemed to have adequate Data Protection. When you get a question asking to explain the principles make sure you explain them and not just state them.Example: Personal data must be fairly and lawfully processed which means that companies must collect personal information with a lawful reason to have the dataOCR are also aware that the law is constantly changing especially in regards to DPA therefore answers will be accepted that use an interpretation of the law based on when the specification was set (2015) or when the examination was sat.E.g. you can include GDPRCompanies can face extremely large fines if they are found to be in breach of the Data Protection ActCompanies must appoint a member of staff as their Data Controller. They will then be responsible for making sure that the principles of the Data Protection Act are not breached and to keep in communication with the Information CommissionerThe company must put in place physical or digital security measures to prevent the data from being accessed without consentThe company should make sure that they train their staff to abide by the principles Companies must send a copy of the subject's data if a Subject Access Request (SAR) is received. This copy must be sent securely after the company has verified the identity of the subjectUnder the Data Protection legislation, data subjects have the following rights with regards to their personal information:To be informed about the collection and the use of their personal dataTo access personal data and supplementary informationTo have inaccurate personal data rectified, or completed if it is incompleteTo be forgotten in certain circumstancesTo restrict processing in certain circumstancesTo data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across different servicesTo object to processing in certain circumstancesTo automated decision making and profilingTo withdraw consent at any time (where relevant)To complain to the Information CommissionerBritish Airways fined £20m over GDPR Breach“British Airways (BA) has been fined £20 million by the UK's data protection authority over data security failings which enabled unauthorised access to be obtained to personal and payment card information relating to more than 400,000 of its customers.” - External link to Pisent Masons articleThings that British Airways could have done to prevent the breach:Making sure that employees have multi-factor authentications on their log-insUsing Role-based controls that allow different users to be assigned different permissions Having a form of efficient and effective security monitoring Regularly penetration testing and fixing any issues that occur promptlyThese are all deemed good practice and would have likely either prevented the attack or enabled British Airways to spot the breach themselves as opposed to being told about it by a third party. Did this page help you? This article needs to be updated. Please help update this article to reflect recent events or newly available information. (July 2018) United Kingdom legislationSerious Crime Act 2015United KingdomLong titleAn Act to amend the Proceeds of Crime Act 2002, the Computer Misuse Act 1990, Part 4 of the Policing and Crime Act 2009, section 1 of the Children and Young Persons Act 1933, the Sexual Offences Act 2003, the Street Offences Act 1959, the Female Genital Mutilation Act 2003, the Prohibition of Female Genital Mutilation (Scotland) Act 2005, the Prison Act 1952 and the Terrorism Act 2006; to make provision about involvement in organised crime groups and about serious crime prevention orders; to make provision for the seizure and forfeiture of drug-cutting agents; to make it an offence to possess an item that contains advice or guidance about committing sexual offences against children; to create an offence in relation to controlling or coercive behaviour in intimate or family relationships; to make provision for the prevention or restriction of the use of communication devices by persons detained in custodial institutions; to make provision approving for the purposes of section 8 of the European Union Act 2011 certain draft decisions under Article 352 of the Treaty on the Functioning of the European Union relating to serious crime; to make provision about codes of practice that relate to the exercise and performance, in connection with the prevention or detection of serious crime, of powers and duties in relation to communications; and for connected purposes.Citation2015 c.9Introduced byLord Taylor of HolbeachTerritorial extent United KingdomDatesRoyal assent3 March 2015Other legislationAmendsProceeds of Crime Act 2002, Criminal Procedure (Scotland) Act 1995, Serious Organised Crime and Police Act 2005, Computer Misuse Act 1990, Serious Crime Act 2007, Serious Organised Crime and Police Act 2005, Policing and Crime Act 2009, Children and Young Persons Act 1933, Sexual Offences Act 2003, Street Offences Act 1959, Female Genital Mutilation Act 2003, Prohibition of Female Genital Mutilation (Scotland) Act 2005, Prison Act 1952, Terrorism Act 2006Amended byInvestigatory Powers Act 2016, Digital Economy Act 2017, Criminal Finances Act 2017, European Union (Withdrawal) Act 2018Status: AmendedHistory of passage through ParliamentText of statute as originally enactedRevised text of statute as amended The Serious Crime Act 2015 is an Act of the Parliament of the United Kingdom.[1] Introduced in June 2014 as part of the Queen's Speech opening the 2014-15 session of Parliament, the Bill was sponsored by the Home Office. It was passed by Parliament on 2 March 2015, and received royal assent on 3 March 2015.[2] The Bill proceeding the Act proposed a 'Cinderella Law' to outlaw causing emotional distress of children,[3] regulate corrupt accountants and other businesses who assist criminal gangs,[4] regulate 'drug cutting agents',[5] and deal with offences related to female genital mutilation, paedophilia, and amend the Terrorism Act 2006. The Serious Crime Act consists of six parts: Proceeds of crime Computer misuse Organized, serious and gang-related crime Seizure and forfeiture of drug-cutting agents Protection of children and others Miscellaneous and general. This part amends the Proceeds of Crime Act 2002 in determining the extent of a defendant's interest in confiscated property, and amends the procedures surrounding costs and court sentencing. This includes amending, defining, or creating regulations on the extent of a defendant's interest in proceeds of crime, the provision of information by third parties, the time-frame and manner of payment, absconding defendants, and connected purposes.[6] This part amends the Computer Misuse Act 1990 in relation to hacking, creating viruses or Trojan Horses, the deliberate act of creating serious risk to computers or computer systems and amends the territorial extent of computer crimes. This includes a new offence of impairing a computer to cause damage, with a 14 years' prison sentence for damage to the economy or environment, in addition to ensuring the United Kingdom adopts the EU Directive 2013/40/EU on attacks against information systems.[6] This part adopts the ratified UN Convention against Transnational Organised Crime. The new 'participation offence' would encompass not just those who carry out an act of serious crime, but those who provide materials, services or related infrastructure. The Bill would extend elements of the Serious Crime Act 2007 to Scotland, and extends the making of a Serious Crime Prevention Order to include firearms offences and the cultivation of cannabis plants.[6] This part creates and extends the power of search and seizure warrants related to the investigation into the creation or ownership of substances used when 'cutting' drugs.[6] This part extends the definition of child cruelty to incorporate abuse, neglect or