**The Computer Misuse Act 1990 – A Discussion**

On the 29th of June 1990, The Computer Misuse Act (CMA) was brought into fruition following the Prestel Scandal (Regina v Gold and Schifreen, 1988) wherein Robert Schifreen and Steve Gold in late 1984 and early 1985 took control of BT's Prestel System and hacked the Duke of Edinburgh's email, in the case of R v Gold and Schifreen, the pair were acquitted post-conviction of their charges due to there not being a relevant law in place to charge them under, thus creating "An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes." (Gov.uk 1990) Today I will be discussing the Computer Misuse Act itself along with the offences detailed under the Act. Looking at historical offences and convictions which will allow a critical assessment of the offences and the efficacy of the Act in today's modern world.

Looking at the primary offences and amendments in the Computer Misuse Act, which are as follows;

Unauthorised access to computer material. (Section 1, Gov.Uk 1990)

Unauthorised access with intent to commit or facilitate commission of further offences (Section 2, 1990)

Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer. Etc (Section 3, 1990)

The act has since been amended a further two times by Police and Justice Act 2006 and the Serious Crime Act 2015 which added the following two offences to the Computer Misuse Act;

Unauthorised acts causing, or creating risk of, serious damage. (Section 3ZA, 2015)

Making, supplying, or obtaining articles for use in offence under section 1, 3 or 3ZA (Section 3a, 2006)

Please note that under the offence of making, supplying, or obtaining articles for use in offence under sections 1, 3, and 3ZA, it is no longer required to have intent, in part due to section 42 of the Serious Crime Act. In addition to this, it is also noteworthy to acknowledge that due to additions from legislation in the Serious Crime Act 2015 (Serious Crime Act, Part 2, 2015), we are now able to convict and give sentencing based on a true reflection of the damage caused by the offences outlined above. It is worth a mention that Lord Hoffman, DPP v McKeown, DPP v Jones ([1997] 2 Cr. App. R. 155, HL, at page 163), first defined a computer as "A Device for storing, processing and retrieving information" and later, the Council of Europe Cybercrime Convention 2001 defined a computer system as any device or a group of interconnected or related devices, one or more of which, pursuant to a programme, performs automatic processing of data. (HMS, 2012)

The first section, unauthorised access to computer material, makes it an illegal act to enter a computer system without permission, or to utilise someone's identification to access a computer for means such as running a program or obtaining data. It is worth mentioning that this still applies if there is no personal gain to be had from the committed offence. Individuals cannot change, copy, or delete a program, nor can they obtain someone else's password. This section ensures a broad area is covered without restrictive parameters in terms of the legalities to allow a more flexible approach to crimes committed as we delve further and further into a technology-based future. The offences under this act come with minimal sentencing, which could be up to two years in prison or a fine, or a combination of the two. In the case of Ellis v DPP, a former student convicted of unauthorised computer use under s.1 (1), despite seeming minor in its scale, was successful, yet brought into question whether judges are qualified enough to make judgements on computer-based crimes if their understanding of technology is limited, this was brought into question again in R v Cropp whereby a decision was brought about based on the judges understanding of computers with the defendant being acquitted (Computer Misuse Act Cases, 2019).

The second section of the Computer Misuse Act, unauthorised access with intent to commit or facilitate commission of further offences, focuses on intent. Gaining access to a computer system with the intent to commit a crime falls under this section. An individual cannot use someone else's login details to send unlawful material (worms, viruses). An individual cannot give out credentials to another being for this purpose. If that were to happen, then the individual in question would be brought up on charges of facilitating a crime. The punishments are much greater here than in s.1 and come with up to 5 years in prison and/or a fine. An example of a s.2 offence is R v Samir Desai (Computer Misuse Act Cases, 2019), whereby Desai, seemingly without motive, illegally accessed an ex-employers network wreaking havoc and disturbance across the board.

The third section of unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer. Etc. An example of a s.3 offence is R v Grant West (Computer Misuse Act Cases, 2019). Under this section a person is guilty if; he/she carries out any unauthorised acts in relation to a computer, and he/she knew at the time of the offence that the act was unauthorised. This section carries the maximum penalties of up to ten years and/or a fine. S.3 covers all activities relating to viruses, worms, trojan horses, corrupted websites, whereas s.1 and s.2 mainly deal with the hacking minus the sabotage and sometimes massive damage caused financially to the intended target. A landmark case in s.3 is DPP v Lennon and relates to being the first recorded criminal proceedings for Denial of Service attacks (DDoS) Lennon was only 16 at the time of the offence. His defence argued that there was no case to answer due to the network already permitting emails, so the many emails sent out by this attack to stop the network were permitted. The presiding Judge Grant agreed and accepted the argument that there was no case to answer. With the prosecution (DPP) not happy with this outcome, they filed an appeal. After considering everything again from another perspective, Lennon was sentenced to two months of electronic tagging curfew.

The Serious Crime Act was introduced in 2015 to further aid in developing an extension and explanation of various acts and, particularly the Computer Misuse Act and its subsection 3ZA, unauthorised acts causing, or creating risk of, serious damage. S.3ZA allows harsher punishments for those that violate this law, with up to life in prison and/or a fine. Section 3ZA covers predominantly areas of national security, the economy, our environment, and damage caused to human life. S.3ZA poses up to 14 years imprisonment and/or a fine. If an offender has caused significant damage to human welfare or national security, the prison term jumps to life imprisonment. Section 3ZA was introduced to aid the Computer Misuse Act for harsher punishments for crimes that did not fit under s.3 alone. Convictions under s.3ZA are still rare.

In section 3a, Making, supplying, or obtaining articles for use in offence under section 1, 3 or 3ZA, the maximum sentence that can be handed out is up to 2 years in prison and/or a fine. The idea behind creating this section is to protect against potential hacker tools. In this case, the prosecution must prove the defendant's intent. An example of an s3a conviction is R v Lewys Stephen Martin (Computer Misuse Act Cases, 2019). Martin carried out DoS attacks on the Oxford and Cambridge university sites and the Kent police website. In addition to this, there were offences pertaining to two individuals and unauthorised use of a PayPal account. He was sentenced under s.1, 2, 3, and 3a to two years imprisonment, and the courts of appeal also upheld this decision.

It is also worth discussing intent, Mens Rea, pronounced as 'mens reya', developed in the early 1600s in the later part of the common law era. It is a fundamental part of criminal law and pertains to someone's intent; mens rea must be proven with all laws requiring intent. An individual's awareness that his or her conduct is criminal, the Latin for mens rea is 'guilty mind'. Before it gets to the stage of courts and hearings, the evidence must first be provided using various methodologies that are not unlike the methods used in gathering evidence from a crime scene. There are background checks, information gathering using various means, including working with Internet Service Providers (ISPs) and Networking companies to obtain valuable information; these activities are required to be obtained legally and are subject to the same laws that we all are and court orders, and permissions must be obtained. Digital forensics is also carried out and involves looking at the original hardware linked to the crime if any. Cyber Crime Scene Investigation has many tools to utilise, including but not limited to; SIFT workstations that allow for examination on various systems of forensic data (Open Source and Free), Sleuth Kits, X-Ways Forensics, CAINE, Bulk Extractor, a tool helping to extract any pertinent information you might need from hardware, Exif Tool, to work on images and videos and its meta data, and Surface Browser, for detecting the infrastructure of companies. There are so many tools out there for forensic specialists to utilise to aid in investigations.

A further consideration is DPP v Bignell is focused on two police officers using their positions of power to gain information that was not used for police work. They had requested information via a police computer operator from the police national computer (PNC), although the police operators carried out their request, they believed the request was for official police duties thus were not charged concerning these offences. The courts maintained that access to the records was authorised even though it was not used for policing activities. The decision brought about strong responses, mainly critical and worrying suggestions of what this could mean for companies hit with "insider hackers". This situation certainly brings forth a need to clarify certain aspects to cover all aspects of potential cyber-crime. The idea of a hypothetical insider hacking their employers' networks, data, and information, remains within the law because they are authorised in that workspace is a concept that is worrying and baffling at the same time. The introduction of the Data Protection Act 2018 has hopefully provided clarity on how information can be legally obtained using a computer and may have been helpful when considering the particular case of DPP v Bignell.

A statement was made in a journal discussing the Computer Misuse Act and its feasibility, "The calls for patience and greater inquiry, in the search for a better strategy, seemed to fall on deaf ears." (NF MacEwan, University of Salford, Manchester, 2011) MacEwan believes that the CMA is a rushed piece of legislation with not enough thought or understanding of Cyberspace and its potential crimes; many instances describe acts of cyber-crime, yet many cybercrimes go unreported and harbour no convictions based on technicalities and loopholes of the CMA. MacEwan states the prosecution rates between 1990 to 2006; of 214 defendants, only 161 were found guilty and convicted. This rate is just over 75% and lacks enforcement, with only two-thirds of s.1 convictions inviting custodial sentencing. There is also said to be hesitation amongst companies to report being hacked for fear of how their weaknesses will be viewed worldwide, especially their clientele.

There is much to consider when looking at the Computer Misuse Act and its usefulness; with the research carried out up to this point, it would seem that the CMA itself is barely fit for purpose, is not functioning how it needs to be, and does not seem to be a deterrent of any kind to cybercriminals. Advancements in technology are significant and must be considered in relation to examining and dissecting this particular law. It was not until the 1980s that computers started to become a staple of a family home, an expensive one at that, with the technological advances allowing more affordable devices today, with people owning as a minimum a computer and a phone, and many of the smart appliances that we use in everyday life, in lighting, cooking, driving, the possibilities are endless. Hypothetically, is the Computer Misuse Act developed in such a way that it too can keep up with the endless evolution of technology? Only time will tell. Cyberspace is different to what technology was in 1990 when the CMA was brought into fruition; it is different now than in 2006 and even compared to 2015. It is constantly evolving, always posing the unknown and more needs to be done to understand Cyberspace and the crimes that are being committed to being able to fully convict wrongdoings without the loopholes that some seem to slip through, without the lax sentencing that seems to be rampant among convictions under the CMA.

**Reference list**

Computer Misuse Act Cases (2019). Computer Evidence - Computer Misuse Act 1990 cases. [online] computerevidence.co.uk. Available at: https://computerevidence.co.uk/Cases/CMA.htm

DPP v McKeown, DPP v Jones ([1997] 2 Cr. App. R. 155, HL, at page 163) (1997). Director of Public Prosecutions v. McKeown and Jones | [1997] 2 Cr App R 155 | United Kingdom House of Lords | Judgment | Law | CaseMine. [online] www.casemine.com. Available at: https://www.casemine.com/judgement/uk/5b46f1ec2c94e0775e7ee308

Gov.uk (1990). Computer Misuse Act 1990 - Introduction. [online] Legislation.gov.uk. Available at: https://www.legislation.gov.uk/ukpga/1990/18/introduction

HMS, S. of S. for F. and C.A. (2012). Convention on Cybercrime. [online] https://www.gov.uk/official-documents. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\_data/file/238194/8309.pdf

Legal Dictionary (2018). mens rea. [online] TheFreeDictionary.com. Available at: https://legal-dictionary.thefreedictionary.com/mens+rea

NF MacEwan, University of Salford, Manchester (2011). The Computer Misuse Act 1990: Lessons from Its past and Predictions for Its Future - University of Salford Institutional Repository. Salford.ac.uk. [online] Available at: https://usir.salford.ac.uk/id/eprint/15815/.

Onyilofor, E. (2014). The Effectiveness or Otherwise of the Computer Misuse Act 1990: Technological Development and Technology Neutrality. [online] papers.ssrn.com. Available at: https://ssrn.com/abstract=2760024

Police and Justice Act (2006). Police and Justice Act 2006. [online] Legislation.gov.uk. Available at: https://www.legislation.gov.uk/ukpga/2006/48/introduction

Regina v Gold and Schifreen (1988). Regina v Gold and Schifreen: HL 21 Apr 1988 - swarb.co.uk. [online] swarb.co.uk. Available at: https://swarb.co.uk/regina-v-gold-and-schifreen-hl-21-apr-1988/

Section 1, Gov. uk (1990). Computer Misuse Act 1990. [online] Legislation.gov.uk. Available at: https://www.legislation.gov.uk/ukpga/1990/18/section/1

Section 2 (1990). Computer Misuse Act 1990. [online] Legislation.gov.uk. Available at: https://www.legislation.gov.uk/ukpga/1990/18/section/2/2015-05-03

Section 3 (1990). Computer Misuse Act 1990. [online] Legislation.gov.uk. Available at: https://www.legislation.gov.uk/ukpga/1990/18/section/3/2015-05-03

Section 3ZA (2015). Computer Misuse Act 1990. [online] Legislation.gov.uk. Available at: https://www.legislation.gov.uk/ukpga/1990/18/section/3ZA/2015-05-03

Serious Crime Act (2015). Serious Crime Act 2015. [online] Legislation.gov.uk. Available at: https://www.legislation.gov.uk/ukpga/2015/9/introduction

Serious Crime Act, Part 2 (2015). Serious Crime Act 2015. [online] Legislation.gov.uk. Available at: https://www.legislation.gov.uk/ukpga/2015/9/part/2/enacted

UKEssays (2018). Issues In Ethical Hacking And Penetration Testing Information Technology Essay. [online] UKEssays.com. Available at: https://www.ukessays.com/essays/information-technology/issues-in-ethical-hacking-and-penetration-testing-information-technology-essay.php#citethis

Yapp, P. (2020). The 30-year-old Computer Misuse Act is not fit for purpose. [online] www.scl.org. Available at: https://www.scl.org/articles/10854-the-30-year-old-computer-misuse-act-is-not-fit-for-purpose