# The Laws Relating to Cybersecurity

The Computer Misuse Act (hereafter referred to as "CMA"), established in 1990, is the only piece of legislation in the UK specifically written with regards to treating digital property as the target of an offence. No consideration is given to crimes committed using digital means to achieve an objective where the target of a perpetrator's actions is not digital property. Given this piece of legislation is now over 20 years old and exists in a landscape that is constantly developing and transforming, should its relevance to real-world scenarios be questioned?

I will be considering whether the CMA is fit-for-purpose using a scenario revolving around a cybersecurity student at Ericht College in Fife named Mark. The full details of the scenario are below, all of which are fictional:

- On the 1st of September Mark attended a College induction, during which the training staff outlined an after-hours access policy for the Queen Mary building, which forms part of the College's Kirkcaldy campus.
- The after-hours access policy explicitly states that after-hours access to the computer labs, located in the Queen Mary building, is prohibited unless a staff member opens the entrance door for a student with the express purpose of allowing them access to the labs.
- At some time between the 1st of September (after Mark had attended his induction session) and the 12th of September, Mark used a Flipper Zero device (used for wireless hacking) to clone the access card signal of a staff member who regularly accompanies students to provide access to the computer labs.
- On the evening of 12th of September, Mark utilised his Flipper Zero device to gain access to the Queen Mary building after hours without being accompanied by a member of staff.
- Once inside the Queen Mary building, Mark explored several restricted areas of the building (e.g., the faculty offices and research labs). He did not access, or attempt to access, any computer resources once inside the building, nor carry out any other malicious activities or theft.
- All his actions were observed by the campus security guard on CCTV.
- Mark's actions were reported by the security guard, resulting in an investigation as part of the college's non-academic disciplinary process. When questioned about his reasoning for his actions, he stated that he was frustrated at the inconvenience of relying on staff to admit entry and that he was simply curious as to what areas he could access once inside the building using his Flipper Zero device.

Using the details of the scenario given above, I will be arguing that the CMA fails to provide adequate legislation for cybercrime (also referred to as computer crime), which Dennis (2023) defines as "the use of a computer as an instrument to further illegal ends", in cases where the target of the offence is not digital. I hope to demonstrate that the lack of definition and poor scope provided within the CMA are not fit-for-purpose in a cyber landscape that continues to develop and grow at a rapid rate.

In considering the legality of Mark's actions and their relation to the CMA, consideration must first be given to the scope and applicability of the CMA. The CMA (1990) details 5 offences that can be committed under its legislation:

1. Unauthorised access to computer material.

2. Unauthorised access with intent to commit or facilitate commission of further offences.

3. Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

3ZA. Unauthorised acts causing, or creating risk of, serious damage.

3A. Making, supplying or obtaining articles for use in offence under section 1, 3 or 3ZA.

As Mark did not access any computer material whilst in the building, no offence under section 1 of the Act has occurred. It cannot be argued that Mark has committed an offence under sections 2 or 3 of the Act as he had no malicious intent before or during his entry to the Queen Mary building. As he did not cause any damage and it cannot be reasonably argued that he was at risk of causing serious damage whilst in the building, an attempt to charge him under section 3ZA would also be inappropriate. Lastly, as section 3A is dependent on an offence having been committed under sections 1, 3 or 3ZA, this offence would also be inapplicable.

Whilst considering each of the offences and its applicability to Mark's actions, it becomes clear that the Act only covers instances where the target of an individual's actions is digital. It fails to cover crimes committed where a digital tool is utilised to achieve an objective. This potentially flawed approach to computer crime can be evidenced in the summary for the Act, which states that its purpose is to "make provision for securing computer material against unauthorised access or modification". The Act makes no mention of the use, illegal or otherwise, of digital devices being used to gain unauthorised access to tangible or intangible artifacts.

Fafinski (2006) examines the Act and its effectiveness against a rapidly evolving cyber landscape where new attack methods and outcomes are constantly being developed. He argues that computer misuse is not equal to criminal law or computer crime. If Mark's actions are considered to be a form of trespass, it could be argued that his actions do constitute a computer crime, however that would not change any earlier conclusions drawn that the CMA is not an applicable piece of legislation in this case.

Comparisons with Mark's actions can be made with those of the perpetrators of so-called relay attacks, where the target is a car that can be accessed using a keyless entry system. During these attacks the perpetrator uses a handheld radio device whilst in the vicinity of the target vehicle, amplifying the signal the car sends to its key fob. When the fob responds, the car will unlock and start, allowing the perpetrator to drive the car away. In contrast to Mark's actions, it could be argued that the car itself is a computer and that by driving it away from its stationary location, and therefore making an unauthorised modification to the data held within the vehicle's system, an offence under section 1 of the CMA has been committed. If this argument could be upheld, further arguments that offences under sections 2, 3 and 3ZA have also been committed could be made. However, on investigating instances of successful apprehension of perpetrators of this type of crime the favoured offence to pursue in these cases is one of conspiracy to steal. Furthermore, in a review of perpetrators convicted under the CMA none of the examined cases concern theft of a car, physical unauthorised entry to a building using digital means, or unauthorised modification to data held in vehicles (Crawford, 2020). This seeming inconsistency between the consequences of the perpetrator's actions and the offence they are charged with could be attributed to confusion experienced by a judge and/or jury around the terminology within the CMA. As argued by Wilson (2019), the lack of definition around key terms (e.g., "computer") could contribute to perpetrators being charged with offences that have a more obvious definition.

When exploring this lack of definition around the key term "computer" within the CMA, consideration should be given to whether the digital lock providing access to the Queen Mary

building could be described as a “computer”. As the CMA itself lacks a definition for the term, further analysis is required of the specifics of the offences to determine whether the lock could be defined as a “computer”. When analysing the offence specifics, the key terms for the application of an offence are “program” and “data”. Unfortunately, no information on the specifics of the door lock workings has been provided, however it would seem logical that the card reader element accessed by Mark’s Flipper Zero device would contain neither program nor data and acts merely as a receiver for information to send on to an access control system for further processing. As such I do not believe it could be argued that the door lock is a “computer”. Furthermore, I would suggest that any attempt to do so would be confusing to a judge and/or jury as previously discussed.

In examining Mark’s actions, consideration should be given as to whether the CMA could be applied if there was any attempt to access a computer after he had accessed the Queen Mary building. It should be noted that, whilst Mark undoubtedly had authorised credentials to access College computers inside the building, his authorised access to them after-hours was dependent on him being admitted by a staff member. This condition of access was a condition he was aware of yet chose to circumvent. Had he accessed a computer whilst inside the building, it could be argued that it was unauthorised access, and that he had therefore committed an offence under section 1 of the CMA. This lack of definition of the word “authorisation” and the complications arising from it are highlighted by Wilson (2019). It is interesting that such a small difference in Mark’s actions could make for a complete reversal of the initial conclusions that the CMA is not sufficient in this instance however, as he did not access a computer after entering the building, this point is for hypothetical consideration only.

Having examined the applicability of the CMA to Mark’s actions and concluding that this legislation is not appropriate in this instance, consideration can be given in regard to the formal response from Ericht College and what actions might be deemed appropriate. As no access to the College’s own policies and procedures has been provided, examples of these in similar institutions should be examined. Analysing the out-of-hours guidance provided by Abertay University reveals a similar suggested arrangement, whereby students are not permitted access to the laboratory facilities unless supervised by a member of staff (Abertay University, 2021). Details of consequences for breaching the guidelines have not been given in the document, nor any information regarding how compliance or acceptance of the guidelines is monitored however Abertay University has a code of conduct for non-academic misconduct that can be examined for details of how misconduct is addressed within the institution. As Mark was investigated as part of the College’s non-academic disciplinary procedures, it could be argued that his actions can be described as “misusing or making unauthorised use of University premises or items of property” as stated within the non-academic misconduct documentation from Abertay University (2022). This document lists the potential actions that the institution may wish to take to address any breaches of the guidelines and vary in severity from an oral reprimand to a recommendation to the Principal that the student be excluded from their course.

Before consideration is given to which of the recommended courses of action (if any) might be appropriate in Mark’s case, further exploration of any legal avenues that Ericht College could pursue should be undertaken, particularly given it has already been concluded that the CMA is not an appropriate piece of legislation here. The Crown Prosecution Service (2019) states that trespass itself is not a crime but that the act of trespass is an essential element for several other statutory crimes, however upon examination of those related statutory crimes, it does not appear that any of them would be applicable to Mark’s actions. Furthermore, section 9 of the Theft Act (1968) defines burglary (of which breaking and entering is the first element) in terms of intent and/or the attempt

to steal, neither of which were present in Mark's actions. Considering these findings it cannot be argued that Mark has committed a crime, and it is highly unlikely that any legal action could or should be taken against him.

Having considered the contents of the Code of Conduct from Abertay University and the outcome of analysis of potentially applicable legislation, I would suggest that following a formal investigation Ericht College issue Mark with a written reprimand for his actions. It is worth noting that no information regarding Mark's age is available, though it could be assumed that he is between 16 and 18 given his actions took place within a college, rather than a university. As such it could be argued that a more severe outcome, including one of legal proceedings, has the potential to be disproportionately damaging to Mark's circumstances, both academic and personal, and could have a negative impact on his academic career (Simon et al, 2003, cited in Nadelson, 2007). Any investigating party might want to consider a more individualised approach for Mark (Walker, 2010), such as offering him the opportunity to accept a "lesser" severity of reprimand (i.e., oral rather than written) when handed out with a revocation of his after-hours-access privileges for a period of time determined by the investigating party. It may also be beneficial to Mark and the College if he were to repeat the Induction Session to ensure he has full comprehension of the College policies and procedures and how they apply to him. Any disciplinary action taken should be issued with the caveat that any repeat breaches of the guidelines, policies, and procedures that Mark is expected to comply with could result in further and harsher action being taken against him, including that of legal proceedings.

Considerations should be given as to what security measures can be taken to prevent instances of unauthorised access to physical buildings for the future. Daniel Bohan (2018) presents several options relating to the access card implementations that could be considered:

- Implement a modern RFID system that supports encryption. Bohan argues that this is the simplest option, but this may not be possible with legacy systems and/or where cost factors are a major factor (Kamaludin, Mahdin and Aberwajy, 2018).
- Use physically unclonable functions (PUFs). Bohan argues that this would render cloning virtually impossible. As with an encryption implementation, the cost and resources required for implementation and maintenance may render this option unsuitable (Shuyu and Limin, 2022).
- Deploy RFID blocking wallets to protect cards from unsolicited RFID transmissions. Bohan suggests that this option may be applicable as a low-cost solution.
- Consider implementing MFA to support the existing RFID authorisation process. This option is supported by Basilio-Ramirez, Perez-Meana and Ponomaryov (2016) however they also highlight concerns around protection of privacy where biometrics are utilised.

Two non-technical controls that could also be considered are the employment of a security guard at the entrance to any sensitive areas (with the post being occupied 24/7), and/or repeat/regular training for all staff and students of the institution.

A full risk assessment and cost benefit analysis of all potential measures should be conducted to determine their suitability. Such assessments would need to assign a cost to a successful attempt to exploit the vulnerability. In Mark's case this would be highly subjective – no physical damage has taken place, no information breach has occurred, and the reputation of the institution is unlikely to suffer as no legal action is being taken against Mark. Taking into consideration the likelihood and frequency of occurrence, as well as the cost incurred to the institution in the event of a successful attempt to exploit the vulnerability (which in Mark's case could be argued to be nothing) it is likely

that the institution may decide that the costs to implement the controls outweigh the benefit that their implementation would result in. As per guidance provided by Mattord and Whitman (2019) this could result in an acceptance of the risk, with no further security measures being implemented.

When implemented, the CMA was written to address the lack of existing legislation that could be used to pursue justice for the victims of crime against intangible (specifically digital) property and to seek to strengthen the UK's defensive position for its own national digital infrastructure. As the technology used by both perpetrators and victims has progressed, the CMA fails to address the wide range of offences that can be committed using a digital tool to commit crimes against non-digital targets. Furthermore, the lack of definition of key terms within the CMA is confusing to members at all levels of the justice system. During a recent public consultation and review that took place (Home Office, 2023), responses were considered from 51 respondents and as a result the legislation is currently undergoing several amendments. Unfortunately, none of these amendments concern the actual use of digital tools for cybercrime, nor do they seek to clarify key definitions within the legislature. I believe that the CMA in its current state is not fit for purpose and that, despite the recent consultation and review, it still fails to address the use of digital tools on non-digital targets or to provide clarity on its scope. It is highly likely that if one or both elements were to be rectified, applying the CMA to Mark's actions could have been entirely appropriate.

# References


Abertay University (2021) *Access (Out of Hours) – Guidance for Staff*. Available at: https://intranet.abertay.ac.uk/docurl/13615 (Accessed: 14 October 2023)

Abertay University (2022) *Code of Student Discipline: Non-academic Misconduct 2022/23*. Available at: https://www.abertay.ac.uk/about/the-university/governance-and-management/freedom-of-information/8-23-information-procedures-on-student-discipline/code-of-student-discipline-non-academic-misconduct/ (Accessed: 14 October 2023)

Bohan, D. (2018) *RFID Cloning: How to Protect Your Business from Physical Infiltration*. Available at: https://ocd-tech.com/2018/06/26/rfid-cloning-how-to-protect-your-business-from-physical-infiltration/ (Accessed: 14 October 2023)

Basilio-Ramirez, J., Perez-Meana, H. and Ponomaryov, V. (2016) 'Multifactor authentication system based on biometrics and radio frequency identification' *2016 9th International Kharkiv Symposium on Physics and Engineering of Microwaves, Millimeter and Submillimeter Waves (MSMW)*, pp. 1-4, doi: 10.1109/MSMW.2016.7538169.

*Computer Misuse Act c. 18*. Available at: https://www.legislation.gov.uk/ukpga/1990/18/contents (Accessed: 14 October 2023).

Crawford, J. (2021) *The computer misuse act and hackers: A review of those convicted under the Act*. Information Security Group, Royal Holloway University. London, Egham, UK. Available at https://regmedia.co.uk/2021/04/12/techreport-jamescrawford.pdf (Accessed: 14 October 2023).

Crown Prosecution Service (2019) *Trespass and Nuisance on Land*. Available at: https://www.cps.gov.uk/legal-guidance/trespass-and-nuisance-land (Accessed: 14 October 2023).

Dennis, M.A. (2023) 'cybercrime' *Encyclopaedia Britannica* in The Authors of Encyclopaedia Britannica (eds.). [Online]. Available at: https://www.britannica.com/topic/cybercrime (Accessed: 14 October 2023).

Fafinski, S. (2006) 'Access denied: Computer misuse in an era of technological change', *The Journal of Criminal Law*, *70*(5), pp.424-442.

Health & Safety (2021) *Access (Out of Hours) - Guidance for Staff*. Available at: https://intranet.abertay.ac.uk/docurl/13615 (Accessed: 14 October 2023).

Home Office (2023) *Review of the Computer Misuse Act 1990: consultation and response to call for information*. Available at: https://www.gov.uk/government/consultations/computer-misuse-act-1990-call-for-information/outcome/review-of-the-computer-misuse-act-1990-consultation-and-response-to-call-for-information#background (Accessed: 15 October 203)

Kamaludin, H., Mahdin, H. and Abawajy, J.H. (2018) 'Clone tag detection in distributed RFID systems', *PloS one*, 13(3), pp. e0193951–e0193951. doi:10.1371/journal.pone.0193951.

Mattord, H.J. and Whitman, M.E. (2019) *Management of information security*. 6th edn. Boston, Massachusetts: Cengage.

Nadelson, S. (2007) *Academic Misconduct by University Students: Faculty Perceptions and Responses*. 4th edn. Ann Arbor, MI: MPublishing, University of Michigan Library.

Shuyu, C. and Limin, Y. (2022) 'A low-overhead PUF for anti-clone attack of RFID tags', *Microelectronics Journal*, 126, p. 105497. doi:10.1016/j.mejo.2022.105497.

Student and Academic Services (2020) *Code of Student Discipline: Non-Academic Misconduct*. Available at: https://www.abertay.ac.uk/media/8983/code-of-student-discipline-non-academic-misconduct.pdf (Accessed: 14 October 2023).

*Theft Act 1968 c. 60*. Available at: https://www.legislation.gov.uk/ukpga/1968/60/crossheading/theft-robbery-burglary-etc/enacted (Accessed: 14 October 2023).

Walker, S.P. (2010) Child accounting and 'the handling of human souls', *Accounting, Organizations and Society*, 35(6), pp.628-657.

Wilson, K. (2019) *Computer (mis) use and the law: what's wrong with the CMA?* PhD thesis. University of Oxford. Available at: https://ora.ox.ac.uk/objects/uuid:f44d4182-a52f-4842-aee0-28faa8b2acc8 (Accessed: 14 October 2023).

# Bibliography

Evans, G.R. (2015) 'The Authority to Discipline Students: Some New Problem Areas', *Education LJ*, p.248.

Information Commissioner's Office (2018) *The Guide to NIS*. Available at: https://ico.org.uk/for-organisations/the-guide-to-nis/ (Accessed 5th October 2023)

Kerr, O.S. (2007) *How to read a legal opinion: a guide for new law students*.