Crime & Cybersecurity

The CMA, hacking and keeping safe

The essential elements of a crime

- An illegal action or omission (Actus Reus)
  - Excludes thoughts but not words (e.g. perjury)
- Intention (Mens Rea)
  - Voluntary or deliberate act
- However
  - Some offences have strict liability (don’t have to prove intention)
  - Simply performing the forbidden act is to offend
  - Often to do with breaking regulations
  - Convicted even without criminal intention, not even criminal negligence

Cyber-dependent crimes

- Cyber-dependent crimes fall broadly into two main categories:
    - Illicit intrusions into computer networks, such as hacking, and
    - Disruption of computer & network functionality, i.e. DOS or DDOS attacks.
- Cyber crimes are committed for many different reasons. For example:
    - Highly skilled individuals/groups who aim to commit crimes;
    - Highly skilled individuals/groups who want to protest, i.e. hacktivists;
    - Low-skilled individuals/groups using cyber tools developed by others;
    - Organised criminal groups;
    - Cyber-terrorists who intend to cause maximum disruption and impact;
    - States and state-sponsored groups launching cyber-attacks on other countries
    - Insiders or employees with privileged access to computers and networks.

Computer Misuse Act 1990

- Section 1: unauthorised access to computer material
  - Must be knowledge that unauthorised & there must be intention to access
- Section 2: unauthorised access with intent to commit further offences
  - As above with intent to commit a serious ‘further’ offence i.e. blackmail
- Section 3: unauthorised acts with intent to impair, or recklessness as to impairing, operation of computer
  - Impair the operation of any computer, prevent or hinder access to a program or data (i.e. DoS attack), impair operation of a program or the reliability of data. Also, s3A creating hacking tools and s.3ZA causing serious damage (to human welfare, the environment, the economy of any country, national security of any country)
- Penalties – fine or up to 2 years (s1), 5y (s2&s3A), 10y (s3), life (s3ZA) in prison

s3A CMA – hacking tools

- Making, possessing, supplying articles for computer misuse.
  - Prosecutors should be aware that there is a legitimate industry concerned with the security of computer systems that generates 'articles' (this includes any program or data held in electronic form) to test and/or audit hardware and software. Prosecutors need to ascertain that the suspect has a criminal intent. (CPS Guidelines, https://www.cps.gov.uk/legal-guidance/computer-misuse#an10)
- Issues to consider
  - Was the article developed primarily and deliberately for wrongdoing?
  - Is it available on a wide-scale commercial basis and sold legitimately?
  - Is it widely used for legitimate purposes?
  - Does it have a substantial installation base?
  - What was the context in which the article was used compared to original purpose

Case example R v Paul McLoughlin

- McLoughlin, wanted free gaming facilities. He used Istealer, password-stealing software, to create a Trojan wrapped in several malware programs. Users were tricked into downloading this, which enabled the defendant to harvest logins of over 100 people.
- A US resident complained to the University that passwords to her online accounts had been compromised.
- Police, working with McAfee and the University of Salford, identified the encrypted details of an FTP server embedded within the malware, which incriminated McLoughlin.
- Charged with making, supplying or obtaining articles for use in an offence under section 1 or 3. 12 months suspended sentence
- First conviction for s3A offence

s3ZA CMA – damage to human welfare

- Causing or risk causing serious damage to human welfare, environment, economy, national security
  - designed to cater for computer misuse, where the impact is to cause damage to, for example, critical national infrastructure and where a higher penalty should be given
  - Here the definition of “critical national infrastructure”, could be understood to be an asset or system which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, i.e. power plants, transport networks or government networks, and the disruption or destruction of which would have a significant impact

CMA prosecution - factors

- Does the institution, company or other body have in place robust and up to date contracts, terms and conditions or acceptable use polices?
- Are employees, students, customers and others made aware of the CMA and what is lawful and unlawful?
- Do employees, students, customers or others have to sign a declaration that they do not intend to contravene the CMA?

Link to Data Protection Act 2018

- DPA 2018 creates several offences in relation to the control and access to data
- Section 144: Creates an offence for a person to intentionally or recklessly make a false statement in response to an information notice
- 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.

Some questions …

Data (Access and Use) Act 2025

- The Data (Use and Access) Act 2025 doesn't directly amend the Computer Misuse Act 1990, but it introduces new offences
- Especially, **creating and sharing deepfakes**, and **the retention of data** for investigations into child deaths
- It also introduces provisions for disclosing information to improve public services, which may include cooperation with law enforcement

DAU Act 2025 enhances CMA 1990:

- **Deepfake offences:** an offence for creating "deepfake" intimate images without consent
- **Data retention for child death investigations:** provides for the retention of information by internet service providers in connection with investigations into child deaths.
- **Cooperation with law enforcement:** provisions for the disclosure of information to improve public service delivery, which can involve data sharing for law enforcement purposes.
- **Possession of data from offences:** allows for action to be taken against those who possess or use data that was obtained through a Computer Misuse Act offence, such as unauthorized access to a computer system.
- **Employee access:** clarifies that an employee is only guilty of an offence if the employer clearly defines the limits of the employee's authority to access a program or data.

The ethics of hacking

- Hacking is conducting technical activities with the intent of exploiting vulnerabilities within a computer system, network or firewall to obtain unauthorised access.
- **Unauthorised hackers** – black-hats, malicious hackers
- **Grey-hat hackers** – exploit security vulnerabilities to spread public awareness that the vulnerability exists.
- **Authorised hackers** – white-hats, ethical hackers, are generally hired to test systems using a range of methods to identify security weaknesses. They don’t steal anything. Have a code of ethics which prohibits them from sharing how they breached security with anyone outside the client organisation

DPA/UK GDPR & cybersecurity

- The DPA/UK GDPR requires that personal data must be processed securely using appropriate technical and organisational measures.
- It does not mandate a specific set of cyber security techniques but expects companies to take ‘appropriate’ action.
- This means identifying and managing risk. What is appropriate for an organisation will depend upon circumstances, as well as the data being processed and therefore the risks posed.

Cybersecurity accountability

- DPA & GDPR focus on explicit accountability for data protection, placing a direct responsibility on companies to prove they comply with the principles of the regulation
- Companies need to commit to mandatory activities such as staff training, internal data audits and keeping detailed documentation if they wish to avoid falling foul of the DPA & GDPR rules.
- Personal data breaches must be reported to the Information Commissioner’s Office without undue delay (if it meets the threshold for reporting) and within 72 hours.

National Cyber Security Centre

- https://www.ncsc.gov.uk/
- Launched in 2016 NCSC provides a service for public and private-sector organisations in relation to cyber security:
    - It is a knowledge hub which distils knowledge into practical guidance for the public
    - Responds to cyber security incidents and works with organisations and the government to reduce harm caused
    - Uses industry and academic expertise to improve the UK’s cyber security capability
    - Reduces risks to the UK by securing public and private sector networks