Tutorial 5 – CMA, security, privacy and anonymity

The Computer Misuse Act 1990 introduced new offences that couldn't previously be prosecuted. It was amended by the Police and Justice Act 2006 (s3 and s3A) and the Serious Crimes Act 2015 (s3ZA). Unauthorised access is defined in s17. The Act is here https://www.legislation.gov.uk/ukpga/1990/18/contents

1. Interpretation of the CMA

    a. How many computers are involved in Section 1(1)? One or more, there is no limit
    b. Does the offence in Section 1(1) require a Mens Rea? Yes – has to know it is unauthorised
    c. What are the implications of Section 1 (2)? Affects those who unlawfully access computers and then go fishing for data/programs to damage, or who damage whatever they find.
    d. Give examples of articles relevant to Section 3A Primarily will be programs designed to gain help people gain unauthorised access – password breaking programs/keyboard logging etc.
    e. Some such tools are known as "duel use" tools. What does this mean? Could be used for two purposes – so a forensic investigator could use a tool to access computers when doing legitimate work for the police, but it could also be used illegally.
    f. Does the CMA apply to (i) external hackers and (ii) internal staff? Yes, it can include staff if they are not authorised

2. Case discussion
    a. [R. v Bow St Magistrates Courts & Allison] Ojomo was a credit analyst for American Express. She could access all customers' accounts but was only assigned certain accounts. She gave information from the other accounts to Allison. This was used to encode other credit cards and supply PIN numbers which could then be fraudulently used to obtain large sums of money from automatic teller machines. Ojomo said "Yes, I know that I was not authorised to access that data but I was authorised to access other data of the same kind."
    Q: Has either Ojomo or Allison has committed an offence? Why? Both committed an offence. Ojomo wasn't authorised, Allison used information that was unlawfully obtained and used it for unlawful access to other people's bank accounts. They conspired to do this together.
    Bow Street Magistrates Court and Allison, Ex Parte Government of the United States of America, R v. [1999] UKHL 31 (8th July, 1999)
    b. A penetration tester, Cuthbert donated £30 on a *Typhoon Haiyan* charity website, but became concerned at its slow response and poor graphics. He felt it might be a "phishing" site that could misuse the name, address and credit card he had supplied. He tested the site with a directory traversal test – he re-formed the URL to see if the security settings on the remote website would allow him access beyond the web root. His attempt was rejected, so he thought no more of the matter. His attempt triggered an alarm in an intrusion detection system (IDS) installed by British Telecom, the directory traversal being an obvious alerting signature. In a police interview, he suggested that the activity was caused by a proxy server which had been part of the ABN Ambro testing environment. When challenged, he told the true story.
        i. Will Cuthbert be prosecuted? Doubtful but possible, he attempted unauthorised access using a URL even though it wasn't successful
        ii. Will he be convicted? If found guilty yes
        iii. What are the consequences? Might be accused of wasting police time, or get a fine under the CMA

    He was prosecuted under section 1 of the CMA given a £400 fine and ordered to pay £600 costs
    The magistrate said he found him guilty with regret. He lost his job and found it hard to find another.
    J. Oates. 2005 Tsunami hacker convicted. http://www.theregister.co.uk/2005/10/06/tsunami_hacker_convicted/

3. CMA consequences
    a. What are the implications of the Computer Misuse Act for an organisation's security? What might organisations have to do to ensure they can take action under the CMA if necessary?

    You have to put security in place, and you have to be clear about who is authorised to access data. Employees and legitimate users need to know the limits of their authorised access.

4. Anonymity online
    a. YikYak was launched in 2013 and closed down in May 2017. It was popular with school and college students. It was closed because the user base was dwindling and it was associated with cyber-bullying. Secret, another anonymous app, shut down in 2015 after many complaints. Secret allowed users to create and use social chat rooms linked only by geographical location. All posts were anonymous. The original motivation was to connect people across campuses, without having to know them. Other anonymous apps include Whisper, Jodel, and Candid.
    In 2014 Mark Andreessen, founder of Netscape, questioned whether it was ethical to invest in such products because of potential negative consequences for users. He said "Investors make choices every day. Many things don't get funded that would make dollars but aren't ethical, moral and/or legal". On the other side of the argument the Whisper CEO said, "How do you decide who to protect and who to out?" Many consider that you should not focus solely on the negative side of a product when deciding about its utility as many apps can be used for bad purposes.
        i. Was there anything illegal about these applications? No
        ii. Is there a place for anonymous apps that allow people to connect with others? Possibly
        iii. Identify an ethical dilemma in this situation Right to privacy vs Right to protection from abuse

Computer Misuse Act 1990 (excerpts)

Section 1

Unauthorised access to computer material

(1) A person is guilty of an offence if

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer, or to enable any such access to be secured;
(b) the access he intends to secure, or to enable to be secured, is unauthorised; and
(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at

(a) any particular program or data;
(b) a program or data of any particular kind; or
(c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall be liable

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;
(b) on summary conviction in Scotland, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;
(c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.

Section 2

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

Section 3 (Amended by Police & Justice Act 2006)

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

Section 3ZA (Amended by Serious Crimes Act 2015)

Unauthorised acts causing, or creating risk of, serious damage

(2) damage is of a "material kind" for the purposes of this section if it is: ... to human welfare in any place ... to the environment in any place ... to the economy of any country ... to the national security of any country

Section 3A (Introduced by Police & Justice Act 2006)

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

(1) A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA.
(2) A person is guilty of an offence if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA.
(3) A person is guilty of an offence if he obtains any article a)intending to use it to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA, or b) with a view to, its being supplied for use to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA.
(4) In this section "article" includes any program or data held in electronic form.

Section 17

(5) Access of any kind by any person to any program or data held in a computer is unauthorised if -

(a) he is not himself entitled to control access of the kind in question to the program or data; and
(b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.