COM6655 Professional Issues
Autumn 2022-23

Computer misuse and computer crime (part 2)

Professor Guy Brown
Department of Computer Science, University of Sheffield
g.j.brown@sheffield.ac.uk

Aims of this lecture

- To explain legal issues associated with software piracy, viruses and hacking.
- To explain the motivation for, and detail of, the Computer Misuse Act 1990.
- To critically assess the role of the Computer Misuse Act in prosecuting computer crime.

Software piracy

Software piracy

- The concept of software piracy is a difficult one for some to grasp because software resembles what economists call a 'public good'.
- Anti-piracy organisations such as FAST mount raids on software pirates, using special search warrants.
- FAST estimate that 30% of all software in use in the UK is infringing, costing the software industry several 100 million pounds per year.
- See http://www.fast.org.uk

IP Crime and Enforcement Report 2021 (IPO)

Year	2016	2017	2018	2019	2020
TMA Found Guilty	443	398	461	401	180
CDPA Found Guilty	47	47	25	23	1

- TMA = Trade Marks Act
  CDPA = Copyright, Designs and Patents Act
- *"The dramatic fall in successful prosecutions under both the TMA and the CDPA must be understood in context. Covid-19 reduced our capacity to mount efficient operations … bottlenecks in processing legal proceedings are only now being unblocked"*

https://www.gov.uk/government/publications/annual-ip-crime-and-enforcement-report-2020-to-2021/ip-crime-and-enforcement-report-2020-to-2021

Fighting software piracy

- Auditing programs can automate the detection of illegally copied software on computer networks.
- Hardware copy-protection 'keys' can be used, but they are unpopular with consumers.
- More and more software is distributed through digital download, allowing registration through a software key system (e.g. iLok)

Legislation applicable to software piracy

- **Copyright, Designs and Patents Act 1988** defines a number of criminal offences;
  - The most serious are for distributing and importing.
- **Forgery and Counterfeiting Act 1981**
  - A disc, tape or other recording medium may be a 'false instrument'.
- **Trade Descriptions Act 1968**
  - Intended to protect consumers from buying inferior goods, e.g. copied software which is being sold as the genuine article.
- **Q: When is copied software inferior to the real thing?**

Viruses and hacking

Viruses

https://www.hp.com/us-en/shop/tech-takes/top-ten-worst-computer-viruses-in-history

- Viruses are programs that are devised to be copied inadvertently.
- They are concealed in other programs or data, and damage or slow the operation of their 'host' systems.

Virus	($billion)	Year
MyDoom	38.0	2004
SoBig	30.0	2003
Klez	19.8	2001
ILOVEYOU	15.0	2000
WannaCry	4.0	2017
Zeus	3.0	2007
Code Red	2.4	2001

Hacking

- Computer hacking is the accessing of a computer system without the express or implied permission of the owner of that computer system.
- Until the Computer Misuse Act 1990 was introduced, taking legal action against hackers could be difficult:
  - Hacking sometimes motivated by curiosity or mischievousness rather than criminal intent.

R v Gold & Schifreen (1988)

Legislation applicable to viruses and hacking

- **Computer Misuse Act 1990**
  - Introduced new offences aimed at viruses and hacking.
- **Investigatory Powers Act 2016**
  - Under section 3(1) it is an offence to intentionally intercept a communication (in the UK) in the course of its transmission by means of a public or private telecommunication system.
- **Data Protection Act 2018**
  - Offences may be committed alongside cyber-dependant crimes. These include knowingly or recklessly obtaining or disclosing personal data, and selling personal data disclosed without consent.

The Computer Misuse Act 1990

New offences introduced by the CMA 1990

1. **Unauthorised access to computer material**, punishable by 12 months imprisonment and/or an unlimited fine;
2. **Unauthorised access with intent to commit or facilitate commission of further offences**, punishable by 12 months/maximum fine on summary conviction and/or 5 years/fine on indictment;
3. **Unauthorised modification of computer material**, punishable by 12 months/maximum fine on summary conviction and/or 10 years/fine on indictment;

S1: Unauthorised access to computer material

- A person is guilty of this offence if he *'...causes a computer to perform any function with intent to secure access to any program or data held in any computer; the access he intends to secure is unauthorised; and he knows at the time when he causes the computer to perform the function that this is the case…'*
  - Aims to deter hackers without requiring any evidence of intention to commit a crime or alter data or programs.
  - The penalty is moderate.
- **Q. What is the significance of the third clause? ("he knows at the time")**

S2: Unauthorised access with intent …

- A person is guilty if he commits an *'...unauthorised access offence with intent to commit an offence to which this section applies; or facilitate the commission of such an offence (whether by himself or any other person)..'*
- Applies to any criminal offence for which the sentence is at least 5 year:
  - E.g. fraud, theft or blackmail.
  - Addresses a more serious form of hacking, in which unauthorised access is gained with intent to commit a further crime.
- The offence may not be completed, e.g. person attempts to gain access to a computer with the intention of blackmail, but doesn't get past login screen.
  - Could still be convicted if it's shown that they intended to secure access, knew access was unauthorised and had intent to commit blackmail.

S3: Unauthorised modification of computer material

- A person is guilty of this offence if '*he does any act which causes an unauthorised modification of the contents of any computer; and at the time when he does the act he has the requisite intent and the requisite knowledge*'.
- The term 'requisite intent' means to:
  - Impair the operation of a computer
  - Prevent or hinder access to a program or data held in any computer
  - Impair the operation of a program or reliability of data
- The intent need not be directed specifically at:
  - A particular computer
  - A particular program or data
  - A particular modification

More about unauthorised modification

- This offence covers four forms of conduct:
  1. Unauthorised erasure of programs or data contained in computer memory or on a storage medium.
  2. The circulation of a virus infected program, with the intention of causing a modification that will impair the operation of the recipient's computer.
  3. Unauthorised addition of a virus to a computer, which will impair the operation of the computer by using up its capacity.
  4. Unauthorised addition of a password to a data file, thereby rendering that data inaccessible to anyone who does not know the password.

R v Paul Bedworth (1993)

- Paul Bedworth acquitted in first trial under the CMA.
- "*Bedworth clearly knew he was breaking the law by hacking after August 1990, when the Computer Misuse Act came into force, but his obsession denied him the freedom of choice to stop.*"

However, …

- Two of Bedworth's friends, Neil Woods and Karl Strickland, pleaded guilty to similar charges under the CMA.
- They both got six months imprisonment.
- In his summing up, judge Michael Harris said:
- '*...if your passion had been cars rather than computers we would have called your conduct delinquent, and I don't shrink from the analogy of describing what you were doing as intellectual joyriding ... hackers need to be given a clear signal by the Courts that their actions will not and cannot be tolerated...*'

Problems with the CMA?

- The Computer Misuse Act 1990 is cautious, reflecting the great care that must be taken when drafting this kind of legislation.
- The CMA addresses most of the areas of computer misuse identified by the Scottish Law Commission report, apart from electronic eavesdropping (addressed by IPA 2016).
- A concern is the meaning of **unauthorised access**.
- What if access is authorised but the function performed is not?

DPP v Bignell (1998)

- Two police officers used police national computer to gain access to details of motor cars they wanted for private purposes unconnected with duties as police officers.
- Charged with unauthorised access under S1 of CMA 1990
  - The magistrate convicted them under S1
  - But their appeals were allowed – their access was authorised?
  - Decision reversed again by the House of Lords.
- Authorisation to access computer material does not extend to accessing computer material for an **unauthorised purpose**.

Another legal question around access

- **You use a computer when a user has left themselves logged on?**

Another legal question around access

- **You use a computer when a user has left themselves logged on?**
- **DPP v Ellis (2001)**
  - Ex-student of Newcastle University. Used non-open access computers to browse websites, when computer left logged on by previous users.
  - Told by admin officer he did not have permission to use non open-access computers.
  - Convicted under S1 of Computer Misuse Act 1990
  - The claim that what he had done was like picking up a discarded newspaper and reading it was rejected.

Does the Act work?

- Small number of convictions under the CMA 1990 so far.
- Data in 2019 showed 422 prosecutions brought under the CMA over the previous decade, with just 45 convictions and 9 custodial sentences.
- In 2019 17,600 offences were recorded but only 57 were tried under the CMA.
- An issue is the labour-intensive nature of cybercrime investigations.

https://www.theregister.co.uk/2019/05/29/computer_misuse_act_prosecutions_analysis/

Security

Guilty of hacking in the UK? Worry not: Stats show prison is unlikely

Just a 16% chance of being banged up for computer misuse

By Gareth Corfield 29 May 2019 at 08:10 16 SHARE ▼

This is not your typical hacker but this trope annoys all the right kind of people

Analysis Nearly 90 per cent of hacking prosecutions in the UK last year resulted in convictions, though the odds of dodging prison remain high, an analysis by *The Register* has revealed.

Government data from the last 11 years revealed the full extent of police activity against cybercrime, with the number of prosecutions and cautions for hacking and similar offences being relatively low.

CMA – a few last words

- The CMA 1990 is an important step in English Law, that protects computer programs and data as legal property under the **criminal** law.
- However:
  - Prevention is better than cure.
  - Staff training around cybersecurity is very important.
  - With the greater use of networks (and home working) more attention needs to be given to restricting and controlling access.
  - Audit departments have a vital role to play.
- Courts appear to be treating computer crime seriously, but few custodial sentences apparently being administered.

Summary

- Prior to the introduction of the Computer Misuse Act 1990, the ability of criminal law to deal with computer crime was limited.
- The Computer Misuse Act was introduced in 1990. It introduces three new offences:
  - Unauthorised access to computer material
  - Unauthorised access with intent to commit or facilitate further offences
  - Unauthorised modification of computer material
- Application of the CMA has met with mixed success.
- A secure system is a better protection against crime than legislation.