

## **COMPUTER MISUSE ACT 1990**

### **Principle**

**Amendment of the Computer Misuse Act 1990 by the Police and Justice Act 2006, in particular:-**

**Section 1 CMA - Unauthorised Access**

**Section 35 of the Police and Justice Act 2006**

**Section 2 CMA – Unauthorised Access with Intent**

**Section 3 CMA – Unauthorised Acts with Intent to Impair**

**Section 3A CMA – Making, supplying or obtaining articles**

### **Introduction**

The Police and Justice Act 2006 received Royal Assent on 8 November 2006. Part 5 of this Act contains amendments to the existing Computer Misuse Act 1990, although these provisions have not yet come into force.

This guidance is to assist Crown Prosecutors and Designated Caseworkers in the use of their discretion in making decisions in computer misuse cases.

### **Main Changes**

The Computer Misuse Act 1990 (CMA) as amended by the Police and Justice Act 2006 will introduce

- Section 3A CMA an offence which penalises the making; supplying or obtaining of articles for use in offences contrary to sections 1 or 3 CMA. (Section 37 of the Police and Justice Act 2006); and
- Increased the penalty for section 1 CMA (Section 35 of the Police and Justice Act 2006).

### **What is a Computer?**

The CMA does not provide a definition of a computer; this is because it was feared that any definition would soon become out of date due to the rapid with which technology develops.

Definition is therefore left to the Courts who are expected to adopt the contemporary meaning of the word. In [DPP v McKeown, DPP v Jones](#) ([1997] 2Cr App R, 155, HL at page 163) Lord Hoffman defined a computer as “a device for storing, processing and retrieving information”.

## **Jurisdiction**

There is jurisdiction to prosecute all CMA offences if there is “at least one significant link with the domestic jurisdiction” (England and Wales)<sup>1</sup> in the circumstances of the case. Section 2(5) defines significant link [<Archbold 23-88 >](#) In the case of [R v Waddon](#) 6 April 2000 the Court of Appeal held that the content of American websites could come under British jurisdiction when downloaded in the United Kingdom. See also [R v Perrin](#) [2002] 4 [Archbold News](#) 2, CA.

## **The offences**

### **Section 1 CMA - Unauthorised Access**

*As amended by section 35 Police and Justice Act 2006 and Schedule 15 of the Serious Crime Act 2007.* [<Archbold 23-87 >](#)

Sections 1 and 2 of the CMA must be read in conjunction with section 17 of the CMA, which is the interpretation section. [<Archbold 23-100 >](#)

A person guilty of an offence contrary to section 1 CMA shall be liable 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. On conviction on indictment to imprisonment for a term not exceeding two years or to a fine or to both.

The intent under section 1 CMA need not be directed at –

1. Any particular program or data;
2. A program or data of any particular kind; or
3. A program or data held in any particular computer

Section 17 gives the interpretation of “unauthorised access” for the purpose of section 1.

The words “any computer” in section 1(1)(a) CMA does not restrict the offence to the situation where the offender uses one computer to secure unauthorised access to another. An offence is also committed where the offender causes a computer to perform a function with intent to secure unauthorised access to any program or data held in the same computer – see [Attorney-General’s Reference \(No 1 of 1991\)](#) [1993] QB 94.

The offence of unauthorised access requires proof of two mens rea elements:

---

<sup>1</sup> See section 4 CMA.

- (1) there must be knowledge that the intended access was unauthorised; and
- (2) there must have been an intention to obtain information about a program or data held in a computer – section 1(2) CMA.

There has to be knowledge on the part of the offender that the access is unauthorised; mere recklessness is not sufficient. This covers not only hackers but also employees who deliberately exceed their authority and access parts of a system officially denied to them.

In the case of [R v Bow Street Magistrates Court and Allison \(AP\) Ex parte Government of the United States of America \(Allison\) \[2002\]2 AC 216](#), where the House of Lords considered whether an employee could commit an offence of securing “unauthorised access” to a computer contrary to section 1 CMA, it was held that the employee clearly came within the provisions of section 1 CMA as she intentionally caused a computer to give her access to data which she knew she was not authorised to access. Their Lordships made it clear that an employee would only be guilty of an offence if the employer clearly defined the limits of the employee’s authority to access a program or data.

In the earlier case of [DPP v Bignell \[1998\] 1 Cr App R8](#), two police officers, who were authorised to request information from the police national computer (PNC) for policing purposes only, requested a police computer operator to obtain information from the PNC which, unbeknown to the operator, was for their own personal use. The Divisional Court held that the two officers had not committed a section 1 unauthorised access offence. The House of Lords in Allison did not over rule the decision in Bignell, but stated that the conclusion of the Divisional Court in the earlier case was probably right. The House of Lord’s went on to say that “it was a possible view of the facts that the role of the officers in Bignell had merely been to request another to obtain information by using the computer. The computer operator did not exceed his authority. His authority permitted him to access the data on the computer for the purpose of responding to requests made to him in proper form by police officers. No offence had been committed under section 1 of the CMA”.

Prosecutors dealing with CMA cases involving employees should assess carefully the employee’s contract of employment together with any surrounding information (for example oral advice given or office practices amongst others) in order to determine whether the employer had clearly defined the limits of the employee’s authority. Such cases normally depend on whether the evidence available demonstrates sufficiently strongly that the conduct complained of was unauthorised. This has to be assessed on a case-by-case basis applying the Code for Crown Prosecutors.

Prosecutors should remember that section 55 of the Data Protection Act 1998, which is punishable by a fine, is in some circumstances an alternative charge to a section 1 CMA offence.

**Section 35 of the Police and Justice Act 2006** increases the penalty for section 1 CMA offence on summary conviction to a maximum of 12 months’ imprisonment or / and a fine and on indictment to a maximum of 2 years’ imprisonment or / and a fine. All CMA offences are either way and no longer have a time limit. The increased penalty only applies to section 1 offences committed after section 35 Police and Justice Act 2006 comes into force<sup>2</sup>.

---

<sup>2</sup> Section 38(2) Police and Justice Act 2006.

## **Section 2 CMA – Unauthorised Access with Intent**

<Archbold 23-88 >

A person can be found guilty of a section 2 offence even if the commission of the further offence is impossible (section 2(4) CMA). A person found not guilty of a section 2 or 3 CMA offence by a jury, can be convicted of a section 1 CMA offence (section 12 CMA).

Section 2(5) states that a person guilty of an offence contrary to section 2 shall be liable-

- on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and
- on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

## **Section 3 CMA – Unauthorised Acts with Intent to Impair**

*As amended by section 36 Police and Justice Act 2006 and Schedule 15 of the Serious Crime Act 2007.* [http://www.opsi.gov.uk/acts/acts2006/ukpga\\_20060048\\_en\\_7#pt5-pb2-11g36](http://www.opsi.gov.uk/acts/acts2006/ukpga_20060048_en_7#pt5-pb2-11g36)

<Archbold 23-89 >

Every act relied upon to prove the section 3 CMA offence must have taken place after section 36 Police and Justice Act 2006 comes into force<sup>3</sup>.

Section 3 CMA should be considered in cases involving distributed denial of service attacks (DDoS<sup>4</sup>), (1) as the term “act” includes a series of acts, (2) there is no need for any modification to have occurred and (3) the impairment can be temporary. In the mail bombing case of *R v Lennon* [2006] EWCH 1201, 11 May 2006, the Divisional Court stated that, although the owner of a computer able to receive e-mails ordinarily consents to the receipt of e-mails, such consent did not extend to e-mails that had been sent not for the purpose of communicating with the owner but for the purpose of interrupting the operation of the system.

A person guilty of an offence contrary to section 3 is liable on summary conviction to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both; or on conviction on indictment, to imprisonment for a term not exceeding ten years or to a fine or to both.

Section 127 Communications Act 2003 is a summary offence punishable by a maximum period of six months imprisonment that can be considered if section 3 CMA is not appropriate.

## **Section 3A CMA – Making, supplying or obtaining articles**

*As inserted by section 37 Police and Justice Act 2006* <Archbold 23-89a >

<sup>3</sup> Section 38(3) Police and Justice Act 2006.

<sup>4</sup> Denial of Service Attacks is aimed at specific Web sites. The attacker floods the webserver with messages endlessly repeated. This ties up the system and denies access to legitimate users.

[http://www.opsi.gov.uk/acts/acts2006/ukpga\\_20060048\\_en\\_7#pt5-pb2-11g37](http://www.opsi.gov.uk/acts/acts2006/ukpga_20060048_en_7#pt5-pb2-11g37)

Section 3A CMA covers making, supplying or obtaining articles for use in offences contrary to sections 1 or 3 CMA. Section 3A deals with those who produce, for example, malicious scripts or software designed to enable modification of television set top boxes. It does not criminalise possession per se unless an intent to use it to commit one of the other offences in section 1 or 3 CMA can be shown. Every act relied upon to prove the section 3A CMA offence must have taken place after section 37 Police and Justice Act 2006 came into force<sup>5</sup>.

A person guilty of an offence under this section is liable on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine or to both; on conviction on indictment, to imprisonment for a term not exceeding two years or to fine or to both.”

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. Some articles will therefore have a dual use<sup>6</sup> and prosecutors need to ascertain that the suspect has a criminal intent.

If the article was supplied in the course or connection with fraud then Prosecutors should consider if their case is also an offence contrary to section 7 and / or section 6 of the Fraud Act 2006. An offence of making or supplying articles for use in frauds contrary to section 7 is punishable by a maximum of 10 years imprisonment and an offence of possession of articles for use in fraud contrary to section 6 is punishable by a maximum of 5 years imprisonment. Each case should be considered based on its own facts. Link to the Fraud Act 2006 [http://www.cps.gov.uk/legal/section8/chapter\\_d.html](http://www.cps.gov.uk/legal/section8/chapter_d.html)

## Guidance

### **Some factors to be taken into account by prosecutors when considering a prosecution under section 3A CMA**

Whilst the facts of each case will be different, the elements to prove the offence will be the same. Prosecutors dealing with dual use articles should consider the following factors in deciding whether to prosecute:

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

---

<sup>5</sup> Section 38(5) Police and Justice Act 2006.

<sup>6</sup> Dual use articles are those that can be used for a lawful or unlawful purpose.

Section 3A (2) CMA covers the supplying or offering to supply an article “**likely**” to be used to commit, or assist in the commission of an offence contrary to section 1 or 3 CMA. “**Likely**” is not defined in CMA but, in construing what is “likely”, prosecutors should look at the functionality of the article and at what, if any, thought the suspect gave to who would use it; whether for example the article was circulated to a closed and vetted list of IT security professionals or was posted openly.

In determining the **likelihood** of an article being used (or misused) to commit a criminal offence, prosecutors should consider the following:

- Has the article been developed primarily, deliberately and for the sole purpose of committing a CMA offence (i.e. unauthorised access to computer material)?
- Is the article available on a wide scale commercial basis and sold through legitimate channels?
- Is the article widely used for legitimate purposes?
- Does it have a substantial installation base?
- What was the context in which the article was used to commit the offence compared with its original intended purpose?

If prosecutors have any questions relating to the application of section 3A CMA please contact the Policy Helpdesk on 020 7796 8471 or by email at [HQPolicy@cps.gsi.gov.uk](mailto:HQPolicy@cps.gsi.gov.uk).

### Relevant Links

<Archbold 23-87 >

<Archbold 23-88 >

<Archbold 23-89 >

<Archbold 23-89a >

<Archbold 23-100 >

[http://www.opsi.gov.uk/acts/acts2006/ukpga\\_20060048\\_en\\_7#pt5-pb2-11g36](http://www.opsi.gov.uk/acts/acts2006/ukpga_20060048_en_7#pt5-pb2-11g36)

[http://www.opsi.gov.uk/acts/acts2006/ukpga\\_20060048\\_en\\_7#pt5-pb2-11g37](http://www.opsi.gov.uk/acts/acts2006/ukpga_20060048_en_7#pt5-pb2-11g37)

[http://www.cps.gov.uk/legal/section8/chapter\\_d.html](http://www.cps.gov.uk/legal/section8/chapter_d.html)