15 COMPUTER MISUSE

After stuyding this short chapter, you should:

- *understand the legal position regarding the misuse of computers and how common offences are handled under the law;*
- *appreciate why the law has had only a limited effect on the extent of computer misuse.*

15.1 THE PROBLEM

In recent years, the public (or, at least, the media) has been much more concerned about the misuse of the internet than about the more general misuse of computers. Nevertheless, crimes committed using computers form a significant proportion of so-called white collar crime and it has been necessary to introduce legislation specifically aimed at such activities. Until 1990, when the Computer Misuse Act was passed, hacking, that is, gaining unauthorised access or attempting to gain unauthorised access to a computer was not in itself an offence. Attempts were made to convict hackers of stealing electricity but the quantity of electricity involved was minute and impossible to measure. Courts were reluctant to convict and, even if a conviction was obtained, the penalty was trivial.

As a result of the Court of Appeal decision in 1988 to uphold the appeal of two people who had hacked into private mailboxes, legislation to tackle computer crime was brought forward remarkably quickly, resulting in the Computer Misuse Act 1990 (CMA). The internet, although becoming widely used for email, was little known to the general public in 1990 and the CMA did not attempt to address issues arising from its misuse. The arrival of the internet and the enormous growth in its importance during the 1990s made it necessary to address some issues, such as denial of service attacks, that were not covered by the CMA, and this was done in the Police and Justice Act 2006, which made several important amendments to the CMA.

It is a good general principle that legislation should not be introduced to deal with special situations that already fall within the purview of more general laws. For this reason, the Computer Misuse Act does not address some topics, in particular computer fraud, which are better dealt with by more general legislation.

15.2 THE COMPUTER MISUSE ACT 1990

The Computer Misuse Act creates three new offences that can briefly be described as unauthorised access to a computer, unauthorised access to a computer with intention

to commit a serious crime, and unauthorised modification of the contents of a computer. We shall look at each of these in more detail below. It is important to note that the offences are committed if either the computer in question or the offender (or both) are in the UK at the time of the offence. This means that someone who hacks into a computer in the UK or infects it with a virus from anywhere in the world is guilty of a criminal offence and can, in principle, be prosecuted in the UK.

Section 1 of the Computer Misuse Act 1990 states that

> a person is guilty of an offence if
>
> 1. he causes a computer to perform any function with intent to secure access to any program or data held in any computer;
> 2. the access he intends to secure is unauthorised; *and*
> 3. he knows at the time when he causes the computer to perform the function that that is the case.

This is called the **unauthorised access** offence. It is punishable by a fine of up to £5,000 or up to six months' imprisonment.

There are several points that need to be emphasised. First, a person can only be guilty of the offence if they intend to gain unauthorised access and know, or should know, that the access is unauthorised. In other words, you cannot be guilty of the offence by accident.

Secondly, the wording of the Act makes it clear that a person who is authorised to access some programs or data on a computer is guilty of the offence if they attempt to gain access to other programs or data to which they are not authorised to have access.

Finally, it is no defence to claim that no harm was done. The attempt to gain unauthorised access itself constitutes the offence.

Section 2 of the Act is concerned with gaining unauthorised access to a computer with the intention of committing a more serious offence. A blackmailer might attempt to gain unauthorised access to medical records, for example, in order to identify people in prominent positions who had been treated for sexually transmitted diseases, with a view to blackmailing them. A terrorist might try to get access to a computer system for air traffic control with a view to issuing false instructions to pilots in order to cause accidents to happen.

The need for this offence arises because, if a criminal is apprehended as a result of unauthorised access before committing the more serious offence, they cannot be prosecuted for the serious offence, even though there may be ample evidence to show what they intended to do. This offence carries a penalty of up to five years imprisonment or an unlimited fine.

Section 3 of the Act states that

> a person is guilty of an offence if

1. he does any act which causes an unauthorised modification of the contents of any computer; and
2. at the time when he does the act he has the requisite intent and the requisite knowledge.

The Act then goes on to explain that

> the requisite intent is an intent to cause a modification of the contents of any computer and by so doing
>
> 1. to impair the operation of any computer;
> 2. to prevent or hinder access to any program or data held in any computer; or
> 3. to impair the operation of any such program or the reliability of any such data.

Furthermore, the Act goes on to make clear that it is not necessary to have any particular computer or any particular program or data in mind. Like the offence under Section 2, this offence carries a maximum penalty of five years imprisonment or an unlimited fine.

It is the offence created by Section 3 that gives the Act its power. For example, it makes each of the following a criminal offence:

- intentionally spreading a virus, worm, or other pest;
- encrypting a company's data files and demanding a ransom for revealing the key required to decrypt it;
- concealed redirection of browser home pages;
- implanting premium rate diallers (that is, programs that replace the normal dial-up code for the computer with the code for a premium rate service).

15.3 AMENDMENTS TO THE ACT

In 2004, the All-Party Parliamentary Internet Group (now part of the All-Party Parliamentary Communications Group), a group of British members of Parliament and members of the House of Lords, carried out a review of the workings of the Computer Misuse Act. It took evidence from a large number of individuals and organisations, including BCS and the IEE (now the IET), many of whom urged the need to extend the Act to include many more specific offences.

The Group concluded that the Act needed comparatively little modification. It recommended an additional offence of 'impairing access to data', which could be used to prosecute the perpetrators of denial of service attacks, which cannot always be prosecuted under Section 3 of the Act. (A denial of service attack is an attack on a website in which it is flooded with so many requests for service that either the links to the site or the site itself are no longer able to respond to legitimate requests. Such attacks have become extremely common.) It also recommended an increase from six months to two years in the maximum prison sentence for the unauthorised access offence. The recommendations of the Group were largely accepted by the Government

and implemented in the Police and Justice Act 2006 (PJA), which made a number of important amendments to the CMA.

First, the penalties for the basic offence of unauthorised access were increased. The maximum penalty on summary conviction (i.e. conviction in a Magistrates' Court) was increased to imprisonment for up to twelve months (six months in Scotland) and/or a fine of up to £5,000. Under the CMA, the basic offence could only be dealt with in a Magistrates' Court. The PJA allows for trial in a Crown Court (i.e. before a judge and jury), with a maximum prison sentence of two years. The main purpose of the change was to make it apparent that Parliament regarded the offence as a serious one. It also had the side-effect of making the offence an extraditable one, that is, for which a person in Britain charged with committing the offence in another country could be sent by a British court to stand trial in that country.

Second the PJA amends the offence defined in section 3 of the CMA so that it covers unauthorised acts with intent to impair, or with recklessness as to impairing (i.e. not caring that they might impair), the operation of any computer, etc. The point of this change is that it removes the requirement that the hacker has modified something. Thus it covers denial of service attacks where the operation of the computer targeted is impaired not by modifying its contents but by flooding it with messages or other requests. The maximum penalty for the new offence on summary conviction is the same as for unauthorised access but on indictment (i.e. in a Crown Court) it is raised to ten years imprisonment and/or an unlimited fine. The maximum penalty is intended to recognise the fact that such attacks may be intended to compromise a nation's security or to damage a large company permanently.

Third, the PJA introduces a new offence of 'making, supplying or obtaining articles for use in computer misuse offences'. This offence is designed to attack the growing market in hackers' tool kits, sets of software tools that facilitate the unauthorised penetration of computer systems. The penalties are the same as for unauthorised access.

15.4 OPERATION OF THE ACT

EXAMPLES OF PROSECUTIONS

The CMA has been used to prosecute a significant number of high-profile cases successfully, as shown in some recent examples:

- On 16 May 2013, at Southwark Crown Court, Ryan Cleary and three other men were sentenced for offences under the Act. During a three-month period in 2011, the group had hacked into the websites of Sony, News International, PBS and Fox, amongst others, and carried out denial of service attacks on the various sites, including those of the UK Serious Organised Crimes Agency and the CIA. It was this group that was responsible for the breach of security at Sony Entertainments, mentioned in Chapter 13 in the

subsection on operation of the Data Protection Act. Cleary was sentenced to 32 months, and two other men to 30 months and 24 months respectively. The fourth, who at the age of 18 was the youngest member of the group, was sentenced to 20 months in a young offenders' institution. Cleary is also awaiting sentence after being found guilty on a separate charge of possessing 172 indecent images of children, which were found on his computer when he was arrested. At the time of writing a fifth member of the group is awaiting sentence in New York.

- James Jeffery hacked into the website of the British Pregnancy Advisory Service and acquired the records of some 10,000 women who had had pregnancies terminated. In April 2012, he was sentenced to 32 months in prison. He had been threatening to publish the information on the web.
- Active Investigation Services was set up by two moonlighting police officers, Scott Gelsthorpe and Jeremy Young, in 1999. It indulged in a wide range of illegal activities, including many that were offences under the CMA. In one instance, they were hired by a waste disposal company to spy on the activities of Environmental Agency staff who were monitoring its activities. Following a tip-off from BT, the firm's offices were raided in September 2004 and 27 people were arrested. Young and Gelsthorpe were given prison sentences of 27 months and 24 months respectively; many other members of staff and others associated with the company received shorter sentences.

Notwithstanding a few such high profile cases, there is a general feeling that given the extent of hacking and the number of viruses and other malware in circulation, these figures are extraordinarily low. In the first 16 years that the Act was in force, only 214 defendants were proceeded against in magistrates' courts in England and Wales under the Act, of whom 161 were convicted. The number of prosecutions brought in Crown Courts would be much lower.

A number of reasons for this low number of prosecutions have been suggested:

- A company that has suffered an attack that constitutes an offence under the CMA will often prefer to avoid the adverse publicity that could result from a trial, particularly since the rules of the court might prevent them rebutting it. A bank, for example, might be reluctant to see an apparent security weakness publicised because this might cause it to lose customers as well as possibly exposing it to the risk of further attacks. In other words, by prosecuting it risks further losses and there is little likelihood of any significant gain.
- Since the police do not have the resources or the expertise to investigate more than a tiny fraction of the cases, the decision to prosecute would almost certainly mean devoting much management time to the case and calling in external experts, whose fees may be high.
- Too many prosecutions under the Act have failed because of legal technicalities.
- Where convictions have been obtained, the sentences imposed have been at the lower end of those that the Act provides for and have not reflected the

seriousness of the offences. Despite the theoretical maximum of a ten year jail sentence, no one has been sentenced to more than 32 months imprisonment for an offence under the Act.

- Far more publicity has been given to cases in which the defendant was acquitted or received a very light penalty than to those in which the defendant was convicted and sentenced appropriately. Thus, for example, in 1993 at Southwark Crown Court, Paul Bedworth, then 18, who had hacked into and made changes to the *Financial Times* database that cost the newspaper £25,000 and had also hacked into systems at the European Organisation for the Research and Treatment of Cancer that resulted in it receiving £10,000 telephone bill, was acquitted on the grounds that he was addicted to hacking. This verdict received a great deal of publicity but much less publicity was given to the fact that two men arrested with Bedworth were each sentenced to six months imprisonment. (The acquittal of Bedworth was widely held to be perverse – the jury seems to have ignored the judge's instructions.)

The well-publicised case of Gary McKinnon served further to muddy the waters. McKinnon admitted gaining unauthorised access to US defence computers from the UK and causing them to become temporarily inoperable, although he denied malicious intent. He claimed that his motivation was to reveal information about free energy and UFOs, which was being deliberately suppressed by the USA. Following indictment in 2002, the US sought his extradition. He fought against this, asking to be tried in the UK, and claiming that, because he was suffering from Asperger's syndrome, it would be a violation of his rights under the European Convention on Human Rights to extradite him to the USA. Every court hearing ruled against him but a massive popular campaign, founded on anti-American feeling and opposition to the 2003 extradition treaty between the UK and the USA, led the Home Secretary to withdraw the extradition order in 2012, and it was subsequently announced that he would not be prosecuted in the UK. Thus a confessed law-breaker, who had committed serious damage to computer systems in a friendly foreign country, was allowed to avoid trial.

15.5 COMPUTER FRAUD

Computer fraud involves manipulating a computer dishonestly in order to obtain money, property, or services, or to cause loss. Most of the techniques that are used are much older than computers. Such tricks as placing fictitious employees on the payroll or setting up false supplier accounts and creating spurious invoices are still the commonest type of fraud, as they were before computers appeared. The introduction of computers has made it possible to carry out more spectacular frauds and, because of the reluctance that many people have to question computer output, has perhaps made it less likely that these will be uncovered. Nevertheless, the offences are the same as before.

The law relating to fraud in England, Wales and Northern Ireland is largely contained in the Fraud Act 2006, which substantially clarified what had been a complicated and confused area of the law. It also removed several technical problems related to cases of fraud where a computer was involved. There is thus nothing special about fraud cases in which a computer has been involved. That having been said, it is important to realise

that the collection and preservation of evidence generated by, or arising from, computer systems requires specialised expertise.

In Scotland, there is and always has been, a single common law offence of fraud and it has not been felt necessary to introduce a statutory offence.

FURTHER READING

The Computer Misuse Act:
www.legislation.gov.uk/ukpga/1990/18/contents

The first three sections are fairly easy to read but the succeeding sections, although necessary, are highly technical (in the legal sense) and relate to questions of jurisdiction and mechanisms for enforcing the Act.

The following articles give a fuller description of the operation of the Act than has been possible in this chapter:

Akdeniz, Y. (1996). 'Section 3 of the Computer Misuse Act 1990: an antidote for computer viruses!'. *Web Journal of Current Legal Issues*. Can be accessed at: http://webjcli.ncl.ac.uk/1996/issue3/akdeniz3.html.

MacEwan, N. (2008) 'The Computer Misuse Act 1990: lessons from its past and predictions for its future.' *Criminal Law Review* 955. Can be accessed at: http://usir.salford.ac.uk/15815/7/MacEwan_Crim_LR.pdf

Cases brought under the CMA rarely involve legal subtleties and are therefore usually only reported in newspapers rather than in law journals. The resulting reports are usually rather superficial. Newspaper reports about the cases mentioned in the section on operation of the Act can readily be found by typing the name of the accused into a search engine. In the case of Gary McKinnon, however, there is a huge amount of material on the internet, most of it biased in one direction or another. Two court judgements that are readily available and which give some idea of the issues can be found at:
www.bailii.org/ew/cases/EWHC/Admin/2009/2021. html
and
www.publications.parliament.uk/pa/ld200708/ldjudgmt/jd080730/mckinn-1.htm