Module: Web Development Issues
Unit: Legal Aspects of Web Development
Lesson: The Computer Misuse Act 1990

Introduction

Before the Computer Misuse Act came in to being, there were a number of cases of law that involved the use of information technology in one form or another. It was largely through the courts' seeming inability to deal with these cases using existing legislation that the Computer Misuse Act made it onto the statute books.

Two of the most important cases are:

knowledge check

Cox v Riley 1986

Riley was a disgruntled employee of Cox. Riley was fired, but before he left, he erased electronic control programs for an electric saw from the saw's printed circuit card. This rendered the card useless. Riley was charged with criminal damage.

Riley was convicted in the magistrates' court but appealed, on the grounds that damage to property had not actually occurred, as a computer program is "intangible" property ("tangible" property is something you can physically pick up and take away).

The appeal court upheld the conviction as it felt there had indeed been damage to property, as "the owner of the saw, which was unquestionably property for the purposes of the statute, had been required to expend time and effort of a more than minimal amount *(in other words, to re-program it)*, in order to restore it to its original condition".

It was this question over whether a computer program can be classed as property, and therefore damaged, that caused the problem. Although Riley was convicted and his conviction upheld, people were increasingly concerned that existing legislation could not deal with crimes involved computers and technology.

R v Gold & Schifreen 1988

Gold and Schifreen were journalists, claiming they wished to expose computer security deficiencies. They successfully hacked into the Prestel computer system operated by British Telecom, (Prestel was a very early e-mail messaging service). Urban legend has it that it was actually the Duke of Edinburgh's account that they hacked into.

Not unnaturally, British Telecom took rather a dim view of this, and the pair was charged under the Forgery and Counterfeiting Act of 1981. This Act provides an offence when a party presents a "false instrument" with the intention that it should be taken as genuine. In this case the false instrument was said to be the customer identity number and password, used by unauthorised people with the intention that the Prestel computer should take it to be genuine.

Gold and Schifreen and were convicted at trial, but the convictions were overturned by the unanimous judgments of the Court of Appeal and the House of Lords. The problem was that the term "instrument" as defined in the Act could include "any disc, tape, soundtrack or other device in or one which information was recorded or stored". As the customer identity number and password would only be held in memory for a very, very short time and then destroyed, it was felt that this was not "recorded or stored" and so did not fit this definition of an "instrument". A second objection was a necessary identification of the Prestel computer as both a source of the deception and its victim. The Lord Chief

Justice was particularly scathing over the use of the Forgery and Counterfeiting Act in this case, stating:

"We have accordingly come to the conclusion that the language of the Act was not intended to apply to the situation which was shown to exist in this case it is a conclusion which we reached without regret. The Procrustean attempt to force these facts into the language of an Act not designed to fit them produced great difficulties for both judge and jury which we would not wish to see repeated... the appellants' conduct amounted in essence... to dishonestly obtaining access to the relevant data bank by a trick. That is not a criminal offence. If it is thought desirable to make it so, that is a matter for the legislature rather than the courts. We express no view on the matter."

Lawyers have suggested that Schifreen and Gold should really have been charged under the Criminal Damage Act.

The Birth of the Computer Misuse Act 1990

Key Points from Cox v Riley & R v Gold

It is worth summarising the key points arising from these two cases.

Cox v Riley

- Riley was charged under the Criminal Damage Act 1971.
- It is an offence under the Act if a person destroys or damages any property belonging to another.
- The crux of case was that Riley erased a computer program from the control card.
- The defendant argued that a computer program is intangible property that therefore could not be damaged.
- The prosecution argued that the control card, which was tangible property, had been left useless and therefore had been damaged.
- The appeal court upheld Riley's conviction, as it felt there had indeed been damage to property.

R v Gold

- Gold and Shifreen charged under Forgery & Counterfeiting Act 1981 - it was argued later that it should have been the Criminal Damage Act.
- The prosecution tried to argue that there was a "false instrument" i.e. the security code.
- The case went all the way to the House of Lords.
- It was ruled that the security code could not be interpreted as a "false instrument".
- The judge's ruling makes great reading and gave impetus to calls for a review of legislation in the light of the increasing use of technology.
- The ruling was taken by many to mean that hacking was not a criminal activity!

Law Commission Review

In the light of these key cases and growing political and public concern about what can be loosely described as "Computer Crime" the Law Commission was instructed to investigate and report on the situation regarding computer crime.

think about it

Would this have happened if Gold and Shifreen had been prosecuted with the right crime?

The Computer Misuse Act was largely based on the findings of the Law Commission Working Paper, Computer Misuse. Unusually, the Act was actually brought in as a result of a private member's Bill, following an apparent reluctance of Parliament to legislate.

The Act covers the subject of unauthorised access, or, as we might refer to it, "hacking", and other problems, including unauthorised modification of data.

top tips

Computer hacking is illegal or unauthorised accessing of a computer system, network or accounts without the permission of the owner of that computer system.

However, the Act has been described as "a flawed piece of legislation", and some consider that it was rushed in as a response to public fears.

group learning activity

Computer Hacking

Use the Discussion Forum to discuss the following with your fellow learners:

- What reasons or motivations may hackers have for hacking into systems?
- Are hackers villains or heroes?
- Some acts of hacking have been described as "harmless". Can hacking ever be completely harmless?

feedback

Bainbridge, D (2004) provides an interesting and thorough discussion of reasons for and effects of computer hacking in his introduction to chapter 29. A summary is given here:

Motivation and Reasons:

- Thrill - being able to outwit the computer's security systems
- Mental challenge
- Proving an enthusiast's skills to himself or his peers
- Sense of achievement
- To commit criminal or terrorist acts
- To steal or destroy information

Heroes:

- Some have said that hackers have done the IT industry a great service by highlighting the security deficiencies in system.
- In 1989 the University of Colorado offered a computer hacking scholarship to increase knowledge and understanding of the area!

Villains:

- Once a hacker has been into a system, the system manager may have a lot of work to do to ensure the hacker has not actually done any damage or left any "time bombs" in the system.
- Once in, they may be tempted to do something wrong.

"Harmless" Hacking:

- Most hacking is no more than a nuisance, but even "innocent" hackers can cause damage accidentally
- Hackers may make it easier for others with more sinister intentions to hack into the system.

Computer Misuse Act 1990

There are three sections to the Act:

knowledge check

Section 1 â€“ â€œThe Basic Hacking Offenceâ€

This section makes it a criminal offence to attempt to obtain unauthorised access to programs or data held on a computer.

1. A person is guilty of an offence if
2. He causes a computer to perform any function with intent to secure access to any program or data held in any computer;
3. The access he intends is not authorised; and
4. He knows at the time when he causes the computer to perform the function that this is the case.
5. The intent the person has to have to commit an offence under this section need not be directed at:-
6. Any particular program or data;
7. Programs or data of any particular kind;
8. A program or data held in any particular computer.

Section 2 â€“ â€œThe Ulterior Intent Offenceâ€

This section concerns using access to a computer in order to commit a further offence.

A person is guilty of an offence under this section if he commits an offence under section 1 above with intent

a. to commit an offence to which this section applies; or
b. to facilitate the commission of such an offence (whether by himself or by any other person);
c. A further offence is one that is punishable with at least five years' imprisonment or where the sentence is fixed by law.

Section 3 â€“ â€œThe Unauthorised Modification Offenceâ€

This section largely replaces the use of the Criminal Damage Act in "intangible property" cases.

A person is guilty of an offence if

a. He does any act which causes an unauthorised modification of the contents of the computer; and

b. At the time when he does the act he has the requisite intent and the requisite knowledge.

The Act does contain some definitions and guidance, but it does not define "computer", "data" or "program". This allows interpretation and development of the application of the law, and allows for development of technology. Some countries have not been so fortunate - in 1986, the US, for example, defined computers to exclude hand-held devices - because they seemed improbable at the time. Now, of course, palmtop computers are very common.

think about it

Consider some of the "hacking" examples you discussed in the previous group learning activity. How could they give rise to charges under the CMA?

Reference Cases under the CMA

Section 1

The Attorney-General's Reference Case, No 1 of 1991

This test case specifically clarifies the meaning of "any computer".

An ex-employee of a wholesaler visited his former employers to purchase some items. While alone, the ex-employee used the shop computer to give himself a large discount on the things he had bought. He did not need a password. He was charged under section 1 of the CMA.

The judge at the original trial said that the wording of section 1 required that a second computer had to be involved. The Attorney-General referred the case to Court of Appeal for clarification on this point of law (the Act had only been on the statute books for a short time).

The Court of Appeal rejected the initial judgment, holding that "the wording in section 1, given its plain and ordinary meaning, was not limited to the use of one computer with intent to gain access to another computer. The offence was made out even if only one computer was used."

top tips

An offence can be committed under the Act even if only one computer is involved.

R v Paul Bedworth

Another important and famous case is that of **Paul Bedworth**, a teenager who was prosecuted for conspiracy to commit offences under sections 1 and 3 of the Computer Misuse Act.

Bedworth hacked into a huge number of computers across Europe, including the Financial Times in London and European Community offices in Luxembourg. The trial judge observed that the full list of computers that had been attacked would be 'as long as a telephone directory'.

Evidence was presented that argued that Bedworth was addicted to computer hacking, to the extent that he became aggressive when he was prevented from using his computer. The defence counsel argued that, although he knew what he was doing was wrong, he could not stop himself. In other words, he was not capable of the *intent* necessary to commit the offences.

Legally, addiction is not a defence to a criminal charge, but the jury acquitted him. Two others charged with him were sent to prison for six months.

Following this case, there were calls for the need to show intent to be removed from the Act.

think about it

Section 1 requires that the accused has "intent" to secure access. Should this requirement be removed in response to the case of Paul Bedworth?

feedback

This is not generally thought to be desirable - removing the requirement to show intent could make careless or incompetent employees liable to criminal prosecution.

Section 2

This section of the Act requires intent to commit a *further* act for which the sentence is fixed by law, or for which the maximum sentence is five years' imprisonment or more, e.g. theft, murder, blackmail and extortion.

For example, say you had hacked into the computer system of a large bank, but did nothing else, you could be prosecuted under section 1 of the Act. If however, you had hacked into the computer system with intent to rob the bank you could be prosecuted under Section 2 of the Act. (Also, if you were then not found guilty of the section 2 offence, you could still be sentenced under section 1.)

Section 2 can be used even if the further offence was not actually completed or even if the second offence turns out to be impossible - it is the *intention* that is important.

One test case here is **R v Pearlstone, Bow Street Magistrates' Court, April 1991**, An ex-employee used his former company's telephone account and another subscriber's account to defraud the computer-administered telephone system and place calls to the United States. You may wish to research this case, and similar ones, further.

Section 3

This section of the Act requires both requisite *intent* and requisite *knowledge*. The concept of "modification" is defined clearly as alteration, erasure or addition of any program or data, but the definition is still wide enough to cover viruses and delayed action time-bombs as well as direct, immediate modification.

The first major prosecution brought under section 3 was **R v Goulden 1992**. In this case, Goulden was a software contractor in dispute with a printing company, Ampersand. Goulden installed a security package on an Apple workstation, which included a facility to prevent access without the use of a password. Goulden made use of this facility as part of his claim for outstanding fees, denying Ampersand access to their machine.

Due to the computerised nature of their printing operations, Ampersand were unable to function for a period of a few days. They claimed £36,000 lost business as a result of Goulden's actions, including £1,000 for a specialist to override the access protection. The court imposed a two-year conditional discharge on Goulden and a £1650 fine.

This section of the Act has sometimes been criticised as it does not appear to allow for any concept of "recklessness". The prosecution would have to show that the defendant *intended* to commit damage. However, reckless damage is often a feature of hacking cases, where the hacker inadvertently deletes and alters files and data during the course of his activities, causing the victim substantial loss.

The Criminal Damage Act of 1971 can be useful for this kind of case. The accused could deny intent and so avoid prosecution under the CMA, but under the 1971 Act, objective recklessness is sufficient to bring a conviction.

knowledge check

To complete this knowledge check activity, see the Knowledge Check section at the end of this lesson.

knowledge check

To complete this knowledge check activity, see the Knowledge Check section at the end of this lesson.

knowledge check

To complete this knowledge check activity, see the Knowledge Check section at the end of this lesson.

my learning space activity

The previous reference cases give you some idea as to how the law is applied in practice.

Consider the following scenarios. How would you interpret them under the CMA? You may need to research the test cases, and others, a little further first.

1. An employee at a medical practice gains unauthorised access computerised medical records to obtain personal information on her new boyfriend.
2. An employee at a medical practice uses computerised medical records to obtain personal information on patients, with the intention of using it to commit blackmail. The employee never actually goes ahead with the blackmail plan.
3. An employee at a company finds the IT manager's PC unattended, has a play out of curiosity, and accidentally erases all the network settings on the system as a result.
4. Trying lots of passwords to gain access to an Electronic Fund Transfer system to obtain money.
5. Hacking into a bank's computer system and changing personal details and passwords of people holding accounts there.
6. A police officer uses the police national computer to track down his ex-wife's new partner.

feedback

1. This would be an offence under s1. Even if the employee was entitled to access the information, this would be an unauthorised use of it.
2. Blackmail is a "further offence" under s2. An offence under s2 is committed even though the blackmail never actually happened. The intention is what counts.
3. This could well be a case where the Criminal Damage Act might be more appropriate - the test would be whether the employee intended to erase the data (which would come under s3) or whether they had simply been reckless.
4. An offence under s2. There is an intention to commit fraud or theft.
5. This is unauthorised modification of data - s3. It would only come under s2 if there was an intention to commit some further crime, perhaps using the passwords found.
6. Section 1 offence - see the similar case of R v Bennett.

Changes to the Computer Misuse Act

Catalysts for Change

Despite the attempt to future-proof the CMA, technological and political changes continue, and the Act is becoming dated. Although the Internet and the world wide web existed in 1990, their possibilities had barely been considered. New crimes, such as website defacement and denial of service attacks, had not even been dreamt of. So many businesses rely on the Internet for their basic operation nowadays, that this kind of attack can have devastating consequences for its victims.

Developments such as the rise in international terrorism have also contributed to calls for the review or replacement of the Act. In 2002, the Computer Misuse (Amendment) Bill was introduced to the House of Lords, but it failed to make it through Parliament.

In 2004 the All Party Internet Group (APIG) (now the All Party Parliamentary Communications Group (apComms)) published a review of the CMA.

The building momentum for change was helped by a case in 2005, known as a "Denial of Service" (DoS) attack.

In this case, a teenage boy walked free from court after allegedly crashing a former employer's email server, with 5 million emails. He was charged under section 3, but the court ruled that the action didn't break the law. The defence claimed that "email servers are designed to receive emails, and what happened did not constitute unauthorised modification".

The judge said that "the computer world has considerably changed since the 1990 Act", and that there was little legal precedent to refer back to. He then ruled that DoS attacks were not illegal under the CMA.

research activity

Use the Internet to research denial of service attacks and website defacement. List a few key examples of such attacks.

What do you think the effect of such attacks can be on an organisation?

The Police and Justice Bill 2006

This Bill contains amendments to the CMA.

- Section 35 increases the penalties for unauthorised access to a computer. Creating a "backdoor" for later unauthorised use is also covered;
- Section 36 replaces CMA Section 3 with a new definition: "Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of a computer, etc." This includes denial of service attacks. Offence can be committed either deliberately or recklessly. The penalty has been increased to a maximum of 10 years. The requirement for "modification" has been removed.

- Section 37 creates a new "hacking tools" offence called "making, supplying or obtaining articles for use in [computer misuse offences]". It states: "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." "Tools" includes software.

Response to the Amendments

In general, the changes are considered to be a step forward, closing loopholes and clarifying the application of the law to new offences. However, there are areas of concern in both section 36 and 37. These have caused a great deal of discussion and concerns amongst IT professionals.

think about it

Why do you think that sections 36 and 37 have caused such a stir in the IT community?

feedback

In section 36, the requirement for modification of data or programs has been replaced with a concept of "impairment".

What constitutes impairment is a subjective judgement and will require clarification. Impairment may also be difficult to prove, since once the problem is rectified, the system will be running normally. Some parties feel that the amendment would have been better to use "modification or impairment" as grounds for an offence.

The issue with section 37 is that hacking "tools" are produced and used by IT professionals to test systems, for performance and security. Those concerned with computer security, such as anti-virus software researchers, use tools which, of necessity, could also be used by hackers. There is concern that the line between lawful and unlawful use is a fine one.

Some people have said that this could mean it is illegal to announce software vulnerabilities, as this could allow a hacker to commit an offence.

There is some reassurance given in that the prosecution would have to prove intent, and also whether the person (in this case the IT professional) believed at the time that the tool would be used for criminal purposes.

However, there remains concern in some quarters that section 37 is a backwards step, and it remains to be seen what effect the changes will have in practice.

my learning space activity

Knowledge Check

Consider the contents of this lesson, and think about how they could apply to your place of work. For instance:

- Do you know of examples of people using their work PC in ways that could possibly fall under the CMA?
- Has your organisation been a victim of hackers or a DoS attack? Suffered a computer virus infection?
- What was the effect? If not, what effect do you think such an attack could have on the business?
- How vulnerable do you think your organisation is to nuisance or malicious computer crime?
- How seriously is the threat taken?
- What steps are in place to prevent such problems occurring?

Knowledge Checks

Module: Web Development Issues
Unit: Legal Aspects of Web Development
Lesson: The Computer Misuse Act 1990

You can contact us on
02476 765 15700
International: +44 (0) 24 765 15700

The Computer Misuse Act 1990 - Page 7

knowledge check

Which of the following points are true of Section 1 of the Computer Misuse Act 1990?

- Must involve at least two computers connected by a network
- Must involve a specific kind of data, e.g. personal data
- Requires an intention to cause damage
- Requires intent to access the computer, network or data
- Offences can cover employees as well as remote hackers

Submit

Please choose which of the answers above are correct.
When you are happy with your choices press the submit button.

You can contact us on
02476 765 15700
International: +44 (0) 24 765 15700

The Computer Misuse Act 1990 - Page 7

knowledge check

Which of the following points are true of Section 2 of the Computer Misuse Act 1990?

- Must involve a further offence taking place
- Applies when there is intent to commit a further offence
- The further offence must actually be possible
- The accused must intend to commit the further offence himself

Submit

Please choose which of the answers above are correct.
When you are happy with your choices press the submit button.

You can contact us on
02476 765 15700
International: +44 (0) 24 765 15700

The Computer Misuse Act 1990 - Page 7

knowledge check

Which of the following points are true of Section 3 of the Computer Misuse Act 1990?

- Requires intent to modify the contents of a computer
- Applies to accidental erasure of data
- The unauthorised modification must be permanent
- Appropriate in the case of someone distributing a computer virus

Submit

Please choose which of the answers above are correct.
When you are happy with your choices press the submit button.

Knowledge Checks - Solutions

Module: Web Development Issues
Unit: Legal Aspects of Web Development
Lesson: The Computer Misuse Act 1990

The Computer Misuse Act 1990 - Page 7

knowledge check

Which of the following points are true of Section 1 of the Computer Misuse Act 1990?

- Must involve at least two computers connected by a network ✗
- Must involve a specific kind of data, e.g. personal data ✗
- Requires an intention to cause damage ✗
- Requires intent to access the computer, network or data ✓
- Offences can cover employees as well as remote hackers ✓

Submit

Please choose which of the answers above are correct.
When you are happy with your choices press the submit button.

You can contact us on
02476 765 15700
International: +44 (0) 24 765 15700

The Computer Misuse Act 1990 - Page 7

knowledge check

Which of the following points are true of Section 2 of the Computer Misuse Act 1990?

- Must involve a further offence taking place ✗
- Applies when there is intent to commit a further offence ✓
- The further offence must actually be possible ✗
- The accused must intend to commit the further offence himself ✗

Submit

Please choose which of the answers above are correct.
When you are happy with your choices press the submit button.

You can contact us on
02476 765 15700
International: +44 (0) 24 765 15700

The Computer Misuse Act 1990 - Page 7

knowledge check

Which of the following points are true of Section 3 of the Computer Misuse Act 1990?

- Requires intent to modify the contents of a computer ✓
- Applies to accidental erasure of data ✗
- The unauthorised modification must be permanent ✗
- Appropriate in the case of someone distributing a computer virus ✓

Submit

Please choose which of the answers above are correct.
When you are happy with your choices press the submit button.