THE
COMPUTER MISUSE ACT (UK)
1990
1990 Computer Misuse Act – In brief

The Act was created to criminalize unauthorized access to computer systems and to discourage the more serious criminals from using a computer to assist in the commission of a criminal offence or from impairing or hindering access to data stored in a computer.

The Act introduced three new criminal offences:
1. Unauthorized access to computer material
2. Unauthorized access to computer material with intent to commit or facilitate commission of further offences.
3. Unauthorized modification of computer material.

Penalties
Unauthorized Access is called a summary offence and penalties are limited to

- 6 months imprisonment and/or a maximum fine of £5000

For other two offences: Unauthorized access with intent… & Unauthorized modification …

- Are more serious and carry jail terms of up to 5 years and unlimited fines
Computer Misuse Act 1990

- Background
- The Act
- Examples
- Changes/Current situation
In the UK, there are two main branches of the law: criminal law and civil law.

Criminal law,

- largely arose because the state wished to forbid or punish behavior that was not in the public interest...
- One motivation for criminal law was the state wished to stop people seeking their own vengeance for wrongs against their families...
- Hence the state prosecutes cases on behalf of the public: “R. versus Jones”, etc.

Civil law,

- is more concerned with peoples’ rights and obligations – Examples: Business contracts, Implied contracts (e.g. supermarket purchases)
- Product liability – satisfactory quality and fit for purpose
- Liability for negligence
Background

- No laws specifically to deal with computer crime prior to 1990 in UK
- Other laws tried instead
- Examples.
  - Cox v Riley 1986 (Criminal Damage Act 1971)
  - R. v Whitely 1990 (Criminal Damage Act 1971)
  - R. v Gold and Another ( Forgery and Counterfeiting Act 1981)
Background - R v Gold [and Schifreen]

- "R. v Defendant" which would be read as "the Crown against the Defendant".
- 1984 – using home computer (together with information obtained looking over someone’s shoulder at a computer convention), Gold and Schifreen successfully hacked into BT, gaining unauthorized access to email accounts – most importantly the Duke of Edinburgh’s.
- Initially convicted (under the Forgery and Counterfeiting Act 1981), they received small fines; they appealed and their appeal was successful.
Because of the royal connection, the case received much publicity.

After the initial ruling, the case went to the court of Appeal and then to the House of Lords.

The specific House of Lords decision 1988 Interpreted to mean that hacking was not a criminal offence.
Defendant released on appeal

Possible Interpretation: No hacking offense
(Or at least no offense under the Forgery and Counterfeiting Act)

Technical aspects of computing, especially telecomputing can have complex effects that previous laws don’t take into account

High publicity - The case of R. v Gold and Another was highly publicized

Mixed aspects of hacking (It may be done for a number of purposes: good fun, serious disruption, malice)

Lead to English Law Commission (ELC) produced report
- Report No.186, Computer Misuse
- Michael Colvin’s (MP) Private Member’s Bill
- This became the Computer Misuse Act 1990
1990 Computer Misuse Act

- Attempts to plug loopholes of other laws:
  - Applies to fraud, hacking, virus-writing
  - And other computer-related crimes...

- Two main principles:
  - If some conduct is criminal, it should be equally criminal if computer technology is used
  - If some conduct is generally not criminal, it should not become so in a computer context
1990 Computer Misuse Act

ARRANGEMENT OF SECTIONS

Computer misuse offences

1. Unauthorised access to computer material.
2. Unauthorised access with intent to commit or facilitate commission of further offences.
3. Unauthorised modification of computer material.

Jurisdiction

4. Territorial scope of offences under this Act.
5. Significant links with domestic jurisdiction.
6. Territorial scope of inchoate offences related to offences under this Act.
7. Territorial scope of inchoate offences related to offences under external law corresponding to offences under this Act.
8. Relevance of external law.

Miscellaneous and general

10. Saving for certain law enforcement powers.
12. Conviction of an offence under section 1 in proceedings for an offence under section 2 or 3.
15. Extradition where Schedule 1 to the Extradition Act 1989 applies.
16. Application to Northern Ireland.
17. Interpretation.
18. Citation, commencement etc.
1990 Computer Misuse Act

1. Unauthorized access to computer material

Described by the Act’s sponsor as ‘simple hacking’ - using a computer without permission. This carries a penalty of up to six months in prison or a £5000 fine, and is tried in a Magistrate's Court.

Involves causing a computer to perform some function.
1990 Computer Misuse Act

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;
   (b) the access he intends to secure 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 on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.
2. Unauthorised access to computer material with intent to commit or facilitate commission of further offences.

Covers actions such as attempting to use the contents of an email message for blackmail. This is a more serious offence, and the penalty is up to five years imprisonment and an unlimited fine.
Unauthorised access with intent to commit or facilitate commission of further offences

(1) A person is guilty of an offence under this section if he commits an offence under section 1 above (“the unauthorised access offence”) 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); and the
       offence he intends to commit or facilitate is referred to below in this section as the further offence.

(2) This section applies to offences—
   (a) for which the sentence is fixed by law; or
   (b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced
       to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the
       restrictions imposed by section 33 of the [1980 c. 43.] Magistrates’ Courts Act 1980).

(3) It is immaterial for the purposes of this section whether the further offence is to be committed
    on the same occasion as the unauthorised access offence or on any future occasion.

(4) A person may be guilty of an offence under this section even though the facts are such that
    the commission of the further offence is impossible.

(5) A person guilty of an offence under this section shall be liable—
   (a) 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
   (b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to
       both.
3. Unauthorised modification of computer material.
   This section covers distributing a computer virus, or malicious deletion of files, as well as direct actions such as altering an account to obtain fraudulent credit.

Both (2) and (3) are tried in front of a jury.
The Act also includes the offences of conspiracy to commit and incitement to commit the three main offences.
Unauthorised modification of computer material

(1) A person is guilty of an offence if—

(a) he does any act which causes an unauthorised modification of the contents of any computer; and

(b) at the time when he does the act he has the requisite intent and the requisite knowledge.

(2) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any computer and by so doing—

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

(c) to impair the operation of any such program or the reliability of any such data.

(3) The intent need not be directed at—

(a) any particular computer;

(b) any particular program or data or a program or data of any particular kind; or

(c) any particular modification or a modification of any particular kind.

(4) For the purposes of subsection (1)(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorised.

(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary.

(6) For the purposes of the [1971 c. 48.] Criminal Damage Act 1971 a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.

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

(a) 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

(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.
Finally, the Act attempts to cover international computer crime.

Someone can be prosecuted in the UK as long as there is at least one 'significant link' with this country. Hacking into a computer in Milan from a terminal in London is illegal (as is hacking into London from Milan)
“Access” means:

- Altering or erasing a program
- Copying it or moving it to a different place
- Using a program or data
- Causing output from the computer

“Output” includes any login messages

- So, you’re accessing a computer, even before you’ve logged-in! (aimed at dial-in scanners)
Hacking

If a hacker does no damage is it a crime?

Hackers might say:

- They’re “testing security”
- They didn’t break in (security was inadequate)

The Act says hacking is a crime

- because companies have to spend time and money checking that no damage was done
Viruses

Writing & distributing viruses is covered by the Act ("...any act which causes unauthorised modification...")

It doesn’t matter if no damage is done
Or if the “damage” is temporary
But this doesn’t discourage virus writers!

- Best defence is good anti-virus software
Examples 1

Scenario 1

- A student hacks into a college database to impress his friends - *unauthorised access*
- Later he decides to go in again, to alter his grades, but cannot find the correct file - *unauthorised access with intent...*
- A week later he succeeds and alters his grades - *unauthorised modification of data*
Examples 2

Scenario 2

- An employee who is about to made redundant finds the Managing Director’s password; logs into the computer system using this and looks at some confidential files - unauthorised access

- Having received his redundancy notice he goes back in to try and cause some damage but fails to do so - unauthorised access with intent...

- After asking a friend, he finds out how to delete files and wipes the main customer database - unauthorised modification
Current Situation
Police and Justice Act 2006

- Doubles the maximum jail sentence for some hacking offences.
- Makes illegal DoS
- Makes possession of some hacking tools illegal

- Gold works as an independent computer security consultant.
Resources

- Wikipedia ‘Computer Misuse Act 1990’ [latest access 12-08-2008]