

## CHAPTER 40

# Offences of fraud and corruption

---

### *Representations express or implied p 1062*

*Place the following text after the first paragraph*

A person may dishonestly represent that he is a person who he is not in order to make a financial gain. In support of that representation he have stolen the identity of the person whom he represents himself to be. The Police and Justice Act 2006, s 13 empowers the Registrar General for England, Wales and Northern Ireland to supply bulk information contained in any register of deaths to the police and other organisations for use in the prevention, detection and investigation or prosecution of offences. It is intended that this information will be useful in cases of identity fraud.

The misuse of computer hardware or software may involve one or more of the offences described elsewhere in this book. For example, a person who falsifies the data in an account held on computer by inputting false information can be convicted of falsification of accounts, contrary to TA 1968, s 17 if he acts with a view to gain or intent to cause loss.

In addition, the misuse of computer hardware or software may involve one or more of three offences under the Computer Misuse Act 1990 (CMA 1990):

- (a) unauthorised access to computer material;
- (b) unauthorised access with intent;;
- (c) acts with intent to impair, or with recklessness as to impairing, operations of a computer, etc.

---

### **Unauthorised access to computer material P 1071**

In relation to the material which appears below this heading, the **Police and Justice Act 2006, s 35 (not currently in force)** contains proposed amendments to CMA 1990, s 1(1) but the Serious Crime Bill currently before Parliament proposes to repeal the amendments. The text is not affected at this stage.

---

### **Unauthorised modification of computer material p 1072**

*Replace the material under this heading with the following new heading and text when the **Police and Justice Act 2006, s 34** comes into force -*

**Unauthorised acts with intent to impair, or with recklessness as to**

## **impairing, operation of computer etc.**

CMA 1990, s 3(1), is substituted by P & JA 2006, s 36 to provide that.:

- (1) A person is guilty of an offence if –
  - (a) he does any unauthorised act in relation to a computer;
  - (b) at the time when he does the act he knows that it is unauthorised; and
  - (c) either subs (2) or (3) below applies.
- (2) This subsection applies if the person intends by doing the act –
  - (a) to impair the operation of any computer;
  - (b) to prevent or hinder access to any program or data held in the computer;
  - (c) to impair the operation of any such program or the reliability of any such data; or
  - (d) to enable any of the things mentioned in paras (a) to (c) above to be done.

However, the Serious Crime Bill proposes the repeal of (d) above so that (d) is unlikely ever to come into force.

- (3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paras (a) to (d) of subs (2) above.
- (4) The intention referred to in subs (2) above, or the recklessness referred to in subs (3) above, need not relate to –
  - (a) any particular computer;
  - (b) any particular program or data; or
  - (c) a program or data of any particular kind.
- (5) In this section –
  - (a) a reference to doing an act includes a reference to causing an act to be done;
  - (b) ‘act’ includes a series of acts;
  - (c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.

Under the revised section, a person commits an offence if he carries out any unauthorised act in relation to a computer knowing that that act is unauthorised and either having one of the intentions set out in subs (2) above, or being reckless in the way described in subs (3).

CMA 1990, s 3, as revised, prohibits all acts which may lead to denial of service by preventing legitimate users of a service access to it. This could be done, for example, by overloading an Internet Service Provider of a website with e-mails. It criminalises the intentional serious hindering of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data. Thus, inter alia, programmes which generate denial of service, or malicious codes such as viruses, are prohibited..

An act is unauthorised if the person whose act causes it is not entitled to determine whether it should be made.. Although the owner of a computer which is able to receive e-mail is ordinarily to be taken to consent to the sending of e-mails to the computer, such implied consent is not without limits. For example, a divisional court has held, it does not extend to e-mails which are not sent for the purpose of communicating with the owner, but are sent as a 'mail bombing campaign' for the purpose of interrupting the proper operation and use of the system.

The 'intent' set out in s 3(2), as revised, is an intent to impair the operation of a computer, to prevent or hinder access to a program or data, to impair the operation of any such program or the reliability of such data, or to enable such things to be done (*but note the comment above in this respect*). An example would be where someone, by misusing or by-passing a password, places in the files of a computer a bogus email pretending that the password holder was the author; such an addition would result in an unauthorised alteration of the contents of the computer and would clearly be done with intent to cause an alteration of the contents, and by so doing, to impair the reliability of the data on the computer. The intent need not be directed at any particular computer program or data, or a particular kind of program or data, or at any particular modification or particular kind of modification.

It is immaterial whether an unauthorised act or any intended effect of it is, or is intended to be, permanent or merely temporary.

*Add this new offence immediately below that set out above when the P & JA 2006, s37 is in force.*

### **Making, supplying or obtaining articles for use in an offence against s 1 or s 3 of the CMA 1990**

P&JA 2006, s 37 inserted a s 3A into CMA 1990. It provides that a person commits an offence in the following three cases ;

- (a) if he makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of an offence against s 1 or s 3;
- (b) if he supplies or offers to supply any article believing that it is likely to be so used;  
or
- (c) if he obtains any article with a view to it being supplied for such use.

The term 'article' includes any program or data held in electronic form.

Where a charge alleges supplying or offering to supply a quantity of articles it will be necessary to prove that charge in relation to a particular article or a particular number of articles. It will not suffice to prove that a person believed that a proportion of the articles was likely to be used in connection with an offence against s 1 or s 3.

The offences are aimed at 'hacker tools' which are increasingly being used in connection with organised crime. As the term 'article' covers any program or data held in electronic form, it covers the supply of a computer password or other means by which a computer system may be accessed.

---

**Search warrants p 1073**

When the Police and Justice Act 2006, Sch 14 is in force delete the material under this heading.