UK COMPUTER MISUSE ACT STRENGTHENS DATA PROTECTION ACT'S SECURITY PROVISIONS

From 29th August, UK computer misuse becomes an offence with stiff penalties, such as five years in prison and an unlimited fine for those successfully prosecuted. The Department of Trade and Industry (DTI) estimate that computer misuse costs UK industry more than £400 a year. But in the 270 cases recorded by the DTI over the last five years, only six cases have come to court and convictions were secured in only three of those cases. Ian Walden reports on the new law which is designed to be complementary to the Data Protection Act.

Legislative revisions and new legislation has been enacted by many industrialised nations over recent years in order to prevent computer crime. Almost every US state, Canada, Sweden and many members of the EEC, including France, have specific legislation to address this expanding area of concern.

Over recent years, attempts have been made through international organisations to achieve a harmonised approach to legislating against computer crime, and prevent the appearance of computer crime havens. In particular:

1. The OECD Report, "Computer-related crime: Analysis of legal policy" (1986) considered the economic implications of such crime;

2. The Council of Europe Recommendation No. R(89) 9 on "Computer-related crime".

Both reports listed the range of offences necessary to achieve a uniform criminal policy.

Origins of the UK's Computer Misuse Act

In the UK, the Computer Misuse Act 1990 passed both Houses of Parliament in June, and came into force on August 29th. The direct origins of the Act are found in the Law Commission report on Computer Misuse (Cm 819, No. 186) published in October 1989; although the Scottish and English Law Commissions had published previous reports and working papers, as well as a Private Members Bill during the previous parliamentary session. In December 1989, Michael Colvin MP introduced a Private Members' Bill, with the tacit support of the government, and closely following the Law Commission's recommendations.

The primary motivation for governmental support was probably a belief that if the UK did not follow the example of many of its European partners, then the UK's position in the European information market could suffer. This is similar to the reason given by the government when it introduced the Data Protection Act (DPA) into Parliament in 1983. At that time the Under-Secretary of State at the Home Office stated that the DPA will "enable our own data processing industry to participate freely in the European market." The fear is that if the UK does not have adequate legal protection for both systems and data, then companies will process elsewhere.

The Computer Misuse Act's main provisions

The Act introduces three new categories of offence:

* "Unauthorised access to computer material" (s.1): this is the basic hacking offence, and is punishable by a fine of up to £2,000 or six months in jail;

* "Unauthorised access with intent to commit or facilitate commission of further offences" (s.2): such as fraud or blackmail; and

* "Unauthorised modification of computer material" (s.3): e.g. by erasing it or planting viruses.

The latter two offences are viewed as the more serious, and can therefore be punished by a jail sentence of up to five years, and an unlimited fine.

Obviously, computer crime has an international dimension, and therefore the Act includes provisions to offer extended protection. In basic terms, prosecutions will be possible where either the accused or the target computer was located within the UK at the time of the offence, or if the "further offences" intended by the accused were to be carried out in the UK.

The principle of "double criminality" is also introduced into the Act. This means, in regard to the second unauthorised access offence, that a person will not be guilty unless it is also a "further offence" under the law of that other country.

The Act (s.14) gives the police the power to obtain a warrant from a circuit judge if it can be shown that there are "reasonable grounds for believing" that unauthorised access, under Section 1, has, or is about to be committed. During its passage through the Commons, there were attempts to give wider powers to the police to monitor communications during investigations into suspected hackers. This would have involved alterations to the Interception of Communications Act 1985, which currently requries Home Office approval. The amendment failed to be adopted, despite support from the police, since it would have raised significant civil liberties issues.

Data protection implications

* The Act places the burden of proof on the prosecution to show that the access was unauthorised. This is obviously much more difficult in the case of internal employees. Therefore, companies will have to establish clear lines of authority for every employee, or it may be difficult to prove that an employee knowingly or intentionally exceeded his authority.

* Companies need to ensure that their computer security and data protection procedures are constantly effective in order to fulfil their obligations with respect to the legislation. Companies will therefore need to carry out regular audits of their information systems: for the Computer Misuse Act, this will include monitoring access attempts and authority levels; for the Data Protection Act, it

will include checking the company information flows against the Register entry.

* During passage of the Bill, attempts were made to add a provision whereby hackers would be able to offer a defence if computer users had not implemented security measures. The amendment failed. However, Michael Colvin, the Act's proposer, has recently stated:

> "If companies do not invest in their own computer security strategy, then they cannot expect the sympathy of the courts when people are charged under the provisions."

Failure by a company to implement "appropriate security measures" to protect personal data from unauthorised access etc., will also be a breach of the Eighth Principle of the UK Data Protection Act 1984.

* The Computer Misuse Act prevents unauthorised access. However, it does not cover use of the computer system for unauthorised purposes, e.g. employees running their own business in company time. However, protection might be offered under the Data Protection Act, which covers the use of personal data for unauthorised (i.e. non-registered) purposes.

Ian Walden is Tarlo Lyons Research Fellow in Information Technology Law at Nottingham Law School, Nottingham Polytechnic, England.

The Computer Misuse Act 1990: Implications for the Business User

is the title of a conference to be held at the Royal Hotel, Nottingham on 19th November, organized by Nottingham Law School. The objectives are:

* To create familiarity with the Computer Misuse Act 1990
* To consider required responses to the Act
* To develop the required administrative procedures

Presentations will include: the terms and implications of the Act; alternative criminal offences available to computer users; its relationship to the Data Protection Act 1984; a review of information security law; the confidentiality of business and client information; international fraud and transborder computer crime. The afternoon will feature workshops.

Speakers will include staff members of the Nottingham Law School: Professor Nigel Savage; Ian Walden; Eric Dumbill; David Thomas; and Peter Casey, Director, Computer Security, Department of Trade and Industry.

Course fee: £160 + VAT = £184. For further information, contact: Dawn Lambert, Commercial Centre, Nottingham Polytechnic, Burton Street Nottingham, NG1 4BU. Telephone: 0602 486 409 Fax: 0602 486 489.