## COMPUTER LAW CHASES COMPUTER CRIME

**Computer security managers must find it ironical that data protection laws and practice often seem to give more attention to rights of access than methods of ensuring an adequate level of security. In addition, in most European countries the law's defences against computer crimes are weak and confused, both in terms of defining the problem and providing adequate remedies. David Goldberg examines the latest attempt to tackle this question: the Scottish Law Commission (SLC) Report on Computer Crime. This report is likely to be influential in the parallel work of England's Commission which is currently studying the subject.**

The use and application of computers and computer technology in the business world - like most others - has dramatically outpaced the clear response of most legal systems. There have been several good attempts to provide comprehensive overviews in particular areas, notably the 1986 OECD Report: Computer - related crime: an analysis of legal policy. However, the recent decision in England in the case of R. v. Schifreen & Gold has shown how exposed computer systems can be. In this case, the defendants hacked into British Telecom's Prestel (videotex) system and gained entry to the electronic mailbox of the Duke of Edinburgh - the Queen's husband.

The position in Scotland, however, has been clarified by the SLC report: Computer Crime No. 106, June 1987. This report is an authoritative and broad survey of the issues which computer misuse can create for the criminal law, and the policy options available. Unlike some other recommendations, the Commission's approach is not to frame a comprehensive computer crime statute. It is rather to focus on a specific activity which is regarded as viable for legal reform and to propose an appropriate draft bill accordingly.

### Types of computer misuse

The report identifies eight categories of computer misuse:-

1. erasure or falsification of data or programs so as to obtain a financial or other advantage.
2. obtaining unauthorised access to a computer.
3. eavesdropping on a computer.
4. taking of information without physical removal.
5. unauthorised borrowing of computer discs or tapes.
6. making unauthorised use of computer time or facilities.
7. malicious or reckless corruption or erasure of data or programs.
8. denial of access to authorised users.

Readers of PL&B may remember that the fourth category, the taking of wnformation without physical removal, featured in the case of Grant v. Procurator Fiscal of Edinburgh (PL&B August '87 p.16). In that case, the Court refused to declare, as a new crime, the dishonest exploitation of confidential information. The Law Commission mirrors that decision, but rather than saying, as the court did, that it was up to Parliament to deal with the matter, it states unequivocally, "we are in no doubt that the taking of information generally should not become an offence."

**The proposed reform**

After arguing the pros and cons of the scope of reform, the report turns its attention to its main, positive reform proposal. This is that two new specific offences should be created:

1. obtaining access to a program or data stored in a computer without authorisation, in order to inspect such data or program, or to add to, alter or corrupt any such data or program for the purpose of:

   * obtaining advantage for himself or another person; or

   * damaging another person's interests.

2. to obtain (similarly without authorisation) access to a program or data, and to damage another person's interests by recklessly altering, corrupting, erasing or adding to such a program or data.

**Commentary**

No reference to any specific mode of communication with the computer is made. This is in order to catch both the offence commonly called "hacking" and also the case of e.g. the unauthorised employee, making direct, physical contact with the computer keyboard. Incidentally, the report recognises the situation of the partially-authorised employee; the offence refers specifically to "...a program or data, or to a part of such program or data, to which the person in question is not authorised to obtain access."

The offence is stated in terms of an intention to bring about, or the coming about, of a certain result. This, the Commission suggests, is more desirable than drafting a general offence of unauthorised access, which would catch hacking, although that activity might not be done with the sort of injurious intent/result the Commission wishes to catch.

**Secret computer-tapping**

One major qualification to the offence is proposed: the report notes the position under the Interception of Communications Act 1985, which authorises, under certain circumstances, the activity of "telephone-tapping." The question arises: should "official investigating authorities, such as the police, ...be authorised to obtain access to a computer without the knowledge or authority of the computer owner?"

The conclusion was supported by all those consulted by the

Commission. It was that the draft offences would not be committed by investigating authorities covertly accessing a computer for the same reasons and under the same procedures as that provided by the above statute for the case of intercepting telephone conversations.

The only exception might be defining the warrant procedure. The justifications for issuing a telephone-tapping warrant are broadly defined as including

(a) the prevention or detection of serious crime and
(b) safeguarding the economic well-being of the U.K.

It is therefore possible to imagine that the use of such powers for "computer-tapping" might well occur more frequently than the "exceptional circumstances" referred to in the report.

**Jurisdiction**

Business and computer-to-computer communication is international but laws operate in separate legal systems. How does this report deal with the question of jurisdiction? As it says: "In relation to Scotland the offender could be in Scotland and the target computer elsewhere, or vice versa." It concludes that there should be jurisdiction in Scotland to try the actual offence in either case.

**The scale of computer crime**

One question often posed - what is the scale of abuse which the SLC's suggested draft law is intended to counter? The SLC report quotes from a 1986 Hogg Robinson Risk Management Services Division report: "Computer assisted fraud and theft will probably cost UK companies £40 million this year."

In December 1987, only a few months after the SLC Report, the Audit Commission for Local Authorities in England and Wales published its third, triennial survey of computer fraud and abuse. The Audit Commission's Chris Hurford (Associated Director Computing and Computer Audit) writes that, "Regrettably, there are still no reliable official statistics on how widespread the problem is or how much financial loss is actually incurred." In any case, the report states, "the central issue" is not how much has been lost, but "why the fraud occurred at all." The Audit Commission polled 1200 public and private sector organisations; 118 incidents of fraud/abuse were reported and the total fraudulent loss suffered was £2.5 million.

In the context of the SLC's proposed offences, it is perhaps interesting to note the Audit Commission's findings on the types of incidents reported. Of the 118:

* 57 related to unauthorised alteration of input;
* 1 to alteration of computerised data;
* 3 to misuse/alteration of program;
* 22 to theft (of data/facilities/software) and unauthorised private work;
* 35 to hacking ("unauthorised access to data and computer facilities" or "sabotage of facilities").

The amount lost attributed to the first category is £2,381,751 and to the last category - £100.

**Future trends**

The likelihood of any specific legislation being enacted only for Scotland is small. However, such progress as there might be is not helped by the different timing of the English and Scottish Law Commissions' reports. The English Law Commission (ELC) has done some preliminary work on this question, but has been held up by the Schifreen/Gold decision, pending its appeal to the House of Lords. It seems that, broadly, the ELC is working on similar issues to its Scottish counterpart, and may issue a consultative document during 1988.

When it does so, it will be worth watching out for its views on whether there should be a requirement to report all computer crime. The Audit Commission argues that devising appropriate precautions or standards is hindered by the lack of reliable information. Other jurisdictions - notably the U.S. - do require such details. It therefore regrets the SLC's report's conclusion that there should not be such a duty because:

(a) there is no general duty to disclose crimes,

(b) deciding what is a "computer crime" is fraught with definitional difficulties,

(c) it is a largely an unenforceable duty (if the loss is concealable so is the failure to report), and

(d) if the losses caused by computer-crime affect the business and should therefore be declared in the shareholders' interests, that suggests that similar activity so affecting the owners of the business should also be declared.

Companies may be relieved with this closely argued conclusion, protecting as it does their freedom of manoeuvre in this notoriously contentious area. But, if it is really the case that it is in the companies' wider interests to have a "punishment to fit the crime," how is that to be forthcoming without their active and full cooperation?

**David J.A. Goldberg is a lecturer in the School of Law, University of Glasgow; and Consultant in Information Law.**