The Interception Legislation Team
Organised and International Crime Directorate
Room 735
Home Office
50, Queen Anne's Gate
LONDON SW1H 9AT

13th August 1999

IMIS Draft Response to the Home Office Consultation Paper on the Interception of Communications in the United Kingdom

Dear Sirs

The attached is a very much a draft response since the timing of the issue of the paper and of the Electronic Commerce Bill with which it inter-relates has meant that we have be unable to consult more widely than among those with a known interest in the issues.

The combined effect of the two pieces of legislation will be that the proposals apply to anyone whose equipment might be used to provide a communications service (including unwittingly). We therefore feel a need to consult far more widely and to subsequently brief our political advisory panel on the issues as perceived by our members. We will be contacting the IS/IT Trade Press for co-operation accordingly.

The potential responsibilities/liabilities of an IS/IT manager whose systems are believed to have been used (whether by staff, contractors or external "hackers") in the course of rerouting criminal traffic are profound. We are particularly concerned that those drafting this legislation (including the relevant sections of the Electronic Commerce Bill) may not appreciate just how profound they are.

The potential cost to legitimate business of breaches of confidentiality in the course of law enforcement access could also be very substantial. This is particularly so if the security of systems in a large user (e.g. in Banking, Insurance, Aerospace, Petrochemicals etc.) is compromised. Smaller users could be rapidly put out of business if the proposals on the offence of "tipping off" really do require the level of subsequent confidentiality implied. The nature and levels of responsibility/liability for similar levels of confidentiality on the part of those responsible for law enforcement also need serious consideration in this context.

Yours sincerely

Philip Virgo
Strategic Advisor
to the
Institute for the Management of Information Systems

Interception of Communications in the United Kingdom
Draft IMIS Response

1. The Institute for the Management of Information Systems (IMIS) is the professional association for IS and IT managers and, as is increasingly the case, for user managers with responsibility for IS and IT systems. There has not been time to mount a full consultation of members but those involved in previous consultations on related issues are concerned that the impact of the proposals on all whose systems have the potential to be used for criminal traffic have not been thought through. More-over the opportunity for a more radical and effective approach to the rapidly growing problems of electronically assisted crime has been missed.

2. In its submission to the House of Commons Trade and Industry Committee Enquiry on Electronic Commerce, the Institute distinguished between those areas where there was widespread agreement on the need for rapid legislation "to ensure that the UK remains among the most attractive places in the world to do business electronically" and those concerned with the interception of communications, where the issues are complex and rushed legislation could be very damaging to the UK economy while still not achieving the objectives of the law enforcement agencies.

3. The continued inclusion of routines to aid the Interception of Communications within the Draft Electronic Communications Bill is most unfortunate. The proposal to also extend to all communications services providers (including "non-public networks") legislation (IOCA) introduced to place the covert interceptions carried out by the Post Office on a statutory basis after the privatisation of British Telecom is not only unworkable but also inadequate and inappropriate for the emerging needs of e-criminal investigation. The combined effects of this proposal and those in the Electronic Communications Bill have ***very*** serious implications for ***anyone*** running a computing or communications system with Internet access.

4. The growth of electronic business and communications and associated criminal activity has far outstripped the ability of current law enforcement structures to cope. In consequence users commonly have to resist electronic crime by the adoption of strong security and use civil law, where practical, to attempt to recoup any losses. This is beginning to have serious effects on confidence in e-commerce, particularly among small firms.

5. Electronic files and communications and the means of protecting or intercepting them are increasingly mass-market commodities. Law enforcement routines designed around aiding secretive access solely for criminal intelligence purposes (as opposed to enabling the collection of evidence for potential use in court) are inappropriate, inefficient and potentially counterproductive for a world in which electronic crime is increasingly "safer" and more lucrative than physical crime and "electronic terrorism" can be equally deadly.

6. The opportunity of the planned review should instead be taken to make the necessary changes to apply the same legal principles on-line as off-line. Access to electronic premises (files and/or communications) should be on a similar basis (i.e. Judicial Warrant) as access to physical premises. Electronically collected evidence should be on, as nearly as practical, a similar footing to physically collected evidence. Proposals to treat electronically encrypted material differently to traditional codes and ciphers arouse major controversy. It would be unfortunate if otherwise desirable legislation were to fall because of this.