Cyber-Rights & Cyber-Liberties (UK)
Faculty of Law
University of Leeds
Leeds LS2 9JT

Director: Mr Yaman Akdeniz (lawya@cyber-rights.org) *Tel: 0498 865116 Fax: 0113 2335056*

3rd August 1999

Open Letter to:

Mr Lou Gerstner
Chairman and Chief Executive Officer
IBM

Sir Peter Bonfield
Chief Executive
BT

Dear Sirs,

UK Government Electronic Commerce Proposals

1. Both BT and IBM have recently been parties to a government sponsored study in the UK that has led to new proposals for the relationship between electronic commerce, encryption and law enforcement. As we are sure you recognise, this is an area where a difficult balance has to be struck between the rights of individuals and the rights of society as a whole.

2. The proposals that have emerged from this work, in which your representatives were involved, are beneficial to the extent that they have removed the immediate threat of key escrow. But worrying provisions remain for government access to decryption keys and these will have serious privacy and civil rights consequences if they persist in their current form. They will, for example, undoubtedly raise grave questions about their compatibility with the Human Rights Act 1998 which incorporates the European Convention on Human Rights into the English Legal System. Moreover, since these proposals are being advocated in the context of electronic commerce, any controversy about them could be very damaging to public confidence in the security and privacy achieved within this domain.

3. The public have a collective right to expect that individuals will co-operate with them as a group to find and deal with others who act against their interests. But, in imposing this obligation on individuals, the public have a duty in return to ensure that what is required of individuals is no more than is absolutely necessary and that any detrimental impact on them is reduced to an unavoidable minimum.

4. In our view, imposing an obligation to decrypt given encrypted texts, in strictly defined circumstances and with clear legal safeguards, meets this mandate. But to go further and require the revelation of decryption keys goes far too far because this could put the wider privacy, safety and security of individuals, and those with whom they exchange information, at serious risk.

5. It is in the nature of modern cryptography that message recipients will possess the only decryption key for some messages and this means that a criminal can send a message to an innocent party that might then become the target of a decryption order. In this situation an innocent and entirely law abiding recipient of a decryption order may be forced to hand over decryption keys that are being used to protect their entire privacy, safety and security, not just those messages that are targets of the order in question. Worse than this, the government's proposals might even prevent them from giving other law abiding people with whom they correspond any indication that such keys have been compromised since this may constitute 'tipping-off', an offence that carries severe criminal penalties. Hence the privacy, safety and security of their colleagues might also be put at risk.

6. Moreover, since it is a criminal offence not to provide a decryption key that the authorities believe is in a person's possession, honest, law abiding citizens may find themselves having to prove that they do not have, and never have had, a key that they know absolutely nothing about. And if they cannot prove this negative - something that is impossible both in practice and in principle - they will be liable to criminal prosecution and imprisonment.

7. We believe that these measures are pernicious and draconian. If implemented there will undoubtedly be occasions when they seriously imperil the safety, security and privacy of entirely honest and law abiding citizens who, through no fault of their own, have the misfortune to find themselves subject to decryption orders. To convert honest, law abiding citizens into criminals when all they have done is to use cryptography to protect themselves is not a step that any truly democratic government would take. And this is not a step that any company with a sense of duty to the UK public should support.

8. Since both IBM and BT were direct parties to the study that has resulted in these proposals, there is a danger that you will be seen to support these plans in full. This perception is much reinforced by the apparently unqualified support offered in press reports attributed to company spokespeople in recent days. In view of the concerns expressed above, however, we urge you to publish a considered opinion on the UK Government's plans in the light of the concerns we express in this letter.

9. It is worth pointing out that the proposed United States SAFE Bill – Security And Freedom through Encryption (SAFE) Act H.R.850 – contains only a 'key holder obligation to decrypt' without government access to keys and without a tipping-off offence. We consider such provisions to be a reasonable and measured response to the threat that encryption poses for law enforcement and find it hard to accept that the UK Government requires more than is proposed within the United States.

10. We urge you, therefore, to qualify your support for the UK Government's electronic commerce proposals by limiting your support for decryption orders to those that impose a key holder obligation to decrypt (with appropriate legal safeguards). We also seek your support in opposing measures that would provide for UK Government access to the personal decryption keys used by UK citizens to protect their privacy, safety and security.

11. We look forward to hearing your reaction to these concerns.

Dr Brian Gladman, Technical Policy Advisor, acting on behalf of
The Board of Cyber Rights and Cyber-Liberties (UK).

Dr Brian Gladman, Technology Policy Adviser
Telephone: +44 (0) 1905 748990
E-mail: brg@cyber-rights.org

Mr Yaman Akdeniz, Director
Telephone: +44 (0) 498 865116
E-mail: lawya@cyber-rights.org

Mr Nicholas Bohm, E-Commerce Policy Adviser
Telephone: +44 (0) 1279 871272
E-mail: nbohm@cyber-rights.org

Professor Clive Walker, Deputy Director
Telephone: +44 (0) 113 2335033
E-mail: law6cw@cyber-rights.org

Dr. Louise Ellison, Deputy Director
Telephone: +44 (0) 118 9875123 (ext: 7507)
E-mail: lawlee@cyber-rights.org