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*

14th June 1999

Open Letter to:

The Right Honourable Tony Blair, PC, MP, The Prime Minister
10 Downing Street
London SW1

Dear Prime Minister,

The Cabinet Office PIU Paper on Encryption and Law Enforcement

1. This is a response from the Board Members of Cyber-Rights & Cyber-Liberties (UK) to the Cabinet Office Paper entitled "Encryption and Law Enforcement" published in May 1999 by the Performance and Innovation Unit.

2. We should say at the outset that we are pleased to see that the Cabinet Office is now considering the Government's policy on encryption. It has been clear for several years that such a change was needed in order to reconcile the different interests of the many departments that are involved.

3. The objectives of the study and the report as set out in your introduction are most welcome. The promotion of electronic commerce promises to bring significant benefits for UK citizens and encryption services, used effectively, can provide the safety, security and privacy that citizens need if they are to have trust in the information handling that is involved. We warmly welcome the Government's commitment to these aims and hope that the outline approach set out in this report can be further developed to provide encryption policies that meet Government aims whilst also commanding the support of industry and private citizens.

4. However, while we welcome this report as an initial step, we are concerned to find that it places too much emphasis on the value of encryption in support of business interests whilst giving insufficient attention to the interests and concerns of consumers and private citizens.

Privacy

5. A significant failing of the report is that it does not adequately recognise the value of encryption for maintaining and improving the privacy of UK citizens by ensuring that their communications and stored personal data are protected from access by others. Although the use of information technology in electronic commerce will offer major new services for consumers, it will also create many new avenues through which the privacy and personal safety of UK citizens could be undermined. If citizens are to have confidence in electronic commerce and in the electronic information handling that this involves it is vital that their privacy is adequately ensured. The use of encryption is now universally seen as a primary way in which this can be achieved.

6. We are concerned that privacy issues are not sufficiently covered in the PIU report and feel that this is the result of an unbalanced view of the value of encryption. In large measure the report is written from a perspective which sees encryption use as a threat to law enforcement rather than a way of improving the safety, security and privacy of law abiding citizens.

7. In an ideal world it would be possible to provide encryption for lawful use whilst denying its benefits to criminals and others with malign intent. In the real world, however, effective encryption of the kind needed to protect the interests of law abiding citizens cannot be provided in a form that prevents criminals also deriving advantages from its use. In this situation Government policy cannot prevent criminal use and should instead aim to ensure that encryption provides net overall benefits for society. The requirement set out at the end of part four of the report that

> "the development of electronic communications, which promises many benefits to businesses and individuals, should not also give assistance to those who are engaged in serious crime"

is hence an ideal but unrealistic policy objective. If such a requirement had been applied to other existing technologies, none could ever have been used for the benefit of society, since they have all pro-

vided benefits for criminals as well. (The private car is just one of innumerable examples.) We therefore urge the Government to give an assurance that its encryption policy objectives are designed to ensure a net benefit for society and not to deny encryption use by law abiding citizens simply because it can also be used by criminals.

Involvement and Consultation

8. In many areas it is possible to have a dialogue between Government and industry without giving separate consideration to the interests of the UK public. This will be true, for example, where either the Government or industry has a clear alignment with public interests to an extent that ensures that these are adequately protected in the processes of policy development.

9. Sadly in the field of encryption policy such an approach is certain to fail since neither the Government nor industry commands the full trust of the public in this area.

10. Successive UK Governments have maintained a long-standing but largely covert policy of protecting the ability of intelligence agencies to freely collect information with scant regard for the impact of such a policy on the safety, security or privacy of UK citizens. This emphasis may have been justified during the Cold War period, but the reaction of informed public opinion to the growing volume of published information about that policy now suggests that it no longer commands widespread public support.

11. A serious consequence of this lack of balance in the formulation of UK Government encryption policy is that many UK citizens do not see the Government as truly acting in their interests – in short they no longer trust the Government in this respect. And in the case of your own Government this lack of trust was greatly reinforced by the sudden and unexplained change of policy on encryption that occurred soon after the last election.

12. UK citizens have even more to fear from an alignment between Government and industry in which their own interests are not independently represented. Historically, telecommunications companies have co-operated 'behind the scenes' with Governments to ensure that agencies of Government can access the private communications of their customers without their consent. Such abuses have been commonplace in telecommunications generally and have even been pursued through international standards bodies, where governments have obtained the support of industry for seriously weakening the encryption provided for telecommunications in order to ensure that it is possible to infringe the privacy of users.

13. For these reasons we are deeply dismayed to find that the study team has, in the main, consulted precisely those organisations that are implicated in such activities. As far as can be seen, no attempt was made to consult or involve civil liberties or public interest organisations. Moreover, the study team has quite consciously excluded such interests during its work, an action that does much to undermine public confidence in its conclusions and recommendations.

14. In our view this major weakness in the policy formulation process must be remedied if the Government is to restore full public confidence in its encryption policies and the way in which they are formed.

A New Approach

15. We welcome, with two major reservations, the proposal for a 'new approach' based on co-operation between Government and industry.

16. Our first reservation is that the activities of the proposed forum and its subordinate bodies will need to be subject to clear lines of public accountability if they are to command the support and confi dence of the UK public.

17. Our second reservation is that the forum must be extended to include representation from consumer organisations, civil liberties and public policy review bodies and from lay members of the public. Without such wider involvement, the forum and its supporting bodies could easily develop into a conspiracy between Government and industry to undermine the interests of private citizens as has occurred in the past (this has happened, for example, in the European Telecommunications Standards Institute, where encryption standards have been deliberately weakened so that the privacy of users could be infringed without their consent).

18. We hence emphasise that our support for the approach now being advocated is conditional on changes being introduced to meet these concerns. In the form currently advocated we could never have confidence in the operation of the bodies envisaged in these proposals.

Legislative Issues

19. We are surprised and concerned about the legislative proposals that the report contains, which seem to us to propose steps that could remove important civil rights and protections.

20. With public key cryptography only message recipients have decryption keys and this means that a guilty party can compromise an innocent party's key by sending them an encrypted message that causes law enforcement authorities to seek access. The key needed for this belongs to the recipient and is almost certain to protect not only the targeted message but many other messages as well. In such circumstances it is surely unjust to impose a requirement to reveal keys on an entirely innocent party who is not involved in any wrongdoing. It should be sufficient for this party to offer a decrypted copy of the targeted message if they are able to do so. The creation of a situation in which a guilty party can put an entirely innocent party at risk in this way is surely not a step that any democratic Government would consciously take.

21. Worse even than this, a guilty party can use a random key to send a message to an innocent party for which the latter has never possessed any decryption key. If faced with a requirement to decrypt this message, or to provide the decryption key, this innocent party would have to prove that they do not possess such a key. For all practical purposes such a proof would never be possible.

22. To impose such an impossible burden of proof on an accused must amount to an infringement of the presumption of innocence embodied under article 6 of the European Convention on Human Rights. This would be contrary to the recently enacted Human Rights Act 1998 and would create a miscarriage of justice by seriously infringing the right to a fair trial because the accused may not be in a position to provide evidence at all.

23. We cannot support such proposals, which we believe would be a serious curtailment of important and well-established civil rights.

Other Concerns

24. In addition to these concerns we also have a number of more detailed observations on these and other points that are set out in the Annex to this letter.

25. We remain ready to work constructively with the Government to seek further evolution of the proposals set out in the PIU report to meet the reservations expressed here.

Mr Yaman Akdeniz, Director, acting on behalf of
The Board of Cyber Rights and Cyber-Liberties (UK).

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

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

Annex – Detailed Comments on the PIU Report on Encryption and Law Enforcement

The observations made here use the headings and numbering of the PIU report

SUMMARY

It is notable that this report considers only the 'economic value' of encryption and fails to identify its important 'social value' in allowing private citizens to protect the privacy of their communications and their stored data. It seems certain that the Government does not want to recognise or promote this use of encryption because it would conflict with its policy of support for the collection of electronic intelligence without the constraints that respect for privacy would impose.

We would like to see the Government accept the recommendations of the Council of Europe and promote encryption for the benefit of privacy (see: Council of Europe Recommendation for the Protection of Privacy on the Internet, No R (99) 5 of the Committee of Ministers to Member States, February 1999, at http://www.coe.fr/cm/ta/rec/1999/99r5.htm)

Recommendations

The removal of key escrow is a welcome development but nothing is said about the equally important need to remove all export controls on civil cryptographic products. The recent relaxation of controls at and below key lengths of 56 and 64 bits are simply not sufficient, since such key lengths are now far too short for serious security use. The US civil authorities intend to introduce a new civil algorithm to replace DES next year with a minimum key length of 128 bits. All major e-commerce software now uses 128-bit encryption and any genuine effort to promote e-commerce will have to remove all restrictions on software operating at such key lengths.

The report omits any consideration of encryption export controls. This is a surprising and serious omission since such controls clearly fall within the study remit and are widely considered to be one of the most serious impediments to the development of electronic commerce. It is difficult to avoid the conclusion that this omission is a deliberate attempt to divert attention away from continuing Government efforts to maintain encryption export controls that are completely inconsistent with its stated wish to promote electronic commerce.

A New Approach Based on Government and Industry Co-operation

In principle this proposal is a good one provided that there are stringent requirements for open public accountability in all aspects of the operation of the forum and the related organisations. In particular the proposed forum should include representatives from civil liberties and public interest bodies in order to ensure that the interests of UK citizens are fully recognised and protected. The failure to consult such bodies during the study was a major omission and one that carries suspicions of a hidden agenda on the part of the Government (or elements within the UK civil service).

International Framework

It is a sad reflection on Government thinking that this clause is framed in this way. Throughout the document the value of encryption is promoted as a negative one except for its role in e-commerce. In fact the widespread use of encryption will help greatly in making cyberspace a better environment for law-abiding citizens. This is not just about finance but also about their privacy and the removal of the ability of others, including some Governments, to access information to which they have no right.

It seems certain that the privacy value of encryption is not covered because it conflicts with the UK Government's policy of protecting and promoting the role of its national intelligence agencies and minimising the constraints under which they operate.

Paragraph 2.3 – Study Remit

Although key escrow is emphasised, the remit clearly extends to 'the current encryption policy'. It is a significant weakness of the report that it fails to meet this wider remit by omitting any consideration of encryption export controls and their impact on electronic commerce. This is a surprising omission since many consider such controls to be the most serious impediment in the development of the electronic marketplace.

Paragraph 2.4 – Methodology

It is notable that this list omits any organisations or individuals that represent civil liberties interests or those of UK private citizens. This is a serious omission and perpetuates a long-standing weakness in the Government's formulation of encryption policy.

Paragraph 2.5

Given the clear mandate to consider encryption policy it would have been sensible to provide a ***full*** public statement of what the Government's policy on encryption actually is. If this had been done it would then have been possible to consider all aspects of this policy and not just those elements that the Government has chosen to discuss.

Paragraph 3.7

This is the only real coverage of the privacy issue and only considers communications. The privacy of personal stored data is not mentioned. Many feel that the move towards electronic commerce and a fully 'connected world' will bring greatly increased opportunities for the unscrupulous to abuse the privacy of those who use such services. There is also a widely held view that current data protection legislation will need to be strengthened to meet this challenge.

These are important considerations in the development of electronic commerce that are completely absent from this report. Given the speed with which the work was done, this may be no more than an oversight but it can also be seen as further evidence of a lack of UK Government commitment to the privacy rights of its citizens.

Paragraph 4.2 – The Importance of Interception for Effective Law Enforcement

We need better information since the statistics given here are not very meaningful. For example, it is not clear:

- how effective interception is in obtaining convictions;
- what proportion of cases would have still been possible without the use of interception;
- how often interceptions are undertaken without achieving anything of value.

Paragraph 4.4

A criminal or terrorist who is alert to covert surveillance will also be alert to covert interception, so it seems unlikely that this part of the argument carries much weight. If it were true the higher cost of other means would be a valuable constraint that would help to ensure that law enforcement actions did not infringe civil liberties.

In practice, however, the costs of interception are low only when the costs of the required interception mechanisms are excluded. To intercept the communications of terrorists and serious criminals requires global interception resources and these involve enormous sums of money (moreover the extent of the accountability involved in operating such systems is very limited).

The analysis of interception costs in this report is both shallow and misleading. Since the end of the Cold War, the intelligence agencies have increasingly sought to justify their existence using law enforcement arguments. Given the impact of terrorism and crime on society, this investment may well be justified, but there is almost no evidence on which the public could reach such a conclusion. What is certain, however, is that adding only a small proportion of the full cost of UK interception resources to each interception would cast serious doubt on the cost-effectiveness argument used here.

It is hard to believe that any report issued in the name of the Prime Minister would seek to secure public support for interception using cost-effectiveness arguments that are as misleading as those presented here.

Paragraph 4.5

The aversion in the Internet Community referred to here derives not from a lack of understanding but just the opposite. This community is very well aware that UK Government has little interest in meeting the privacy concerns of its citizens, almost certainly because this conflicts with its policy of promoting the collection of intelligence information without the constraints that respect for privacy would impose.

The last sentence is meaningless since it is absolutely inevitable that electronic communications will benefit those involved in serious crime. In practice Government cannot deny these benefits to criminals without also denying them to law-abiding citizens. In consequence, the best the Government can do in this situation is to ensure that there is net benefit for society.

Paragraph 4.10 – The Impact on Interception of Developing Encryption Technologies

There is no published evidence to indicate that this problem is urgent. The evidence that is available suggests that encryption poses no serious problems for law enforcement at the moment. For example, it appears that the Government can quote only a few cases out of many, many thousands of criminal

investigations where encryption has even been a factor, let alone an insurmountable one; and those cases relate to stored data, not intercepted communications. The recent announcement by the German Government states clearly that encryption is not a problem for criminal prosecution and investigation in Germany – it seems most implausible that the situation is very different in the UK.

It is notable that the Government appears admit here that products such as PGP actually provide strong encryption. If this is true both UK citizens and the Government should now be able to use these products in place of the variety of solutions that the UK Government and the UK civil service have been advocating. On the other hand, if these products offer only weak security, then the Government has nothing to worry about since they will not undermine the effectiveness of warranted intercepts.

Paragraph 5.1 – Government Encryption Policy

This coverage of the Government's encryption policy is very incomplete – there needs to be a full, open statement of the Government's policy on encryption and the reasons for it. And this needs to be followed by a careful analysis of the policy and its objectives to see whether its aims are both justified and achievable. Significant aspects of the policy are not being revealed in this paper.

Paragraph 5.2 and 5.3 – Public Key Cryptography

It is notable that this description of public key cryptography is oriented towards the certification of keys by third party Certificate Authorities (CAs). However, cryptography will often be used in situations where two parties can exchange their keys without recourse to third parties, hence avoiding the additional security vulnerabilities that these introduce.

Paragraph 5.4 to 5.6 – Digital Signatures

Again the model is a 'CA model', only one of the possible models and not the best in many practical situations. Moreover, the analysis provided here is shallow since it only covers confidence in public key ownership and says nothing about the more difficult task of managing private key components.

Paragraphs 5.7 to 5.12 – Key Escrow and Licensing

It is disappointing to see no reference to the widespread public disquiet about the Government's 'key escrow friendly' policy. Again there is too much emphasis on the interests of business and too little on the interests of UK citizens.

Paragraph 6.2 – The Merits Of Key Escrow

This analysis is misleading because it provides a set of absolute statements about the possible value of 'key escrow'. What matters, however, is the relative value of key escrow when compared with alternative means of achieving the same objectives. When such relative comparisons are made key escrow fares poorly.

Paragraph 6.3

What would matter is not adoption or implementation but the extent to which escrowed encryption services would be used. Given their serious security vulnerabilities it is doubtful that many would have taken them up.

Paragraph 7.3 – A Government/Industry Joint Forum

"…. This co-operation would need to be based on trust between the parties. …."

AND PUBLIC TRUST IN THESE PARTIES AND THE ACTIONS THEY TAKE.

Although the proposal made here has considerable merits, the failure to set a requirement for open public accountability is a serious flaw. Changes hence need to be introduced that will allow the public to develop trust and confidence in the operation of the proposed forum. In particular:

- the forum and the associated organisations need to be fully and openly accountable to the public;
- the forum needs to include representation from consumer, civil liberties and public interest organisations and lay members of the public.

Paragraph 7.5 – An Encryption Coordination Unit in The Home Office

The concept of an 'encryption co-ordination unit' within the Home Office is a thoroughly bad idea. It is Home Office pressure that has led to the recent effort to promote key escrow and this shows how out of touch the Home Office is with both public and industry concerns in this area. Given this lack of understanding it makes no sense to put the Home Office in the driving seat. This responsibility should continue to rest with the Cabinet Office.

Paragraph 7.7 – Legislative Issues

The proposals made here are a potentially very dangerous infringement of civil rights.

When Public Key Cryptography is used it is possible that an innocent message recipient can be put in jeopardy by a third party simply by sending them an encrypted message. An innocent party might then be forced to compromise their privacy by handing over their secret decryption keys. In this circumstance it should be sufficient for the party to offer the decrypted text, not their keys.

It would also be easy for someone to send a message to another person using a random private key. The innocent party would then have to prove that they don't have a key to decrypt this message. How this could be done is impossible to imagine: no objective evidence could be capable of proving this negative.

To impose an impossible burden of proof on an accused must inevitably amount to an infringement of the presumption of innocence embodied in the European Convention on Human Rights, which would be a significant breach of one of the United Kingdom's most important international obligations.

The right to a fair trial under article 6 of the European Convention of Human Rights incorporated by the Human Rights Act 1998 includes "the right of anyone charged with a criminal offence ... to remain silent and not to contribute to incriminating himself." (See *Funke v. France* (1993) 16 E.H.R.R. 297).

Furthermore, the European Court of Human Rights reiterates that the right of any "person charged" to remain silent and the right not to incriminate himself are generally recognised international standards which lie at the heart of the notion of a fair procedure under Article 6 of the European Convention on Human Rights. Their rationale lies, inter alia, in protecting the "person charged" against improper compulsion by the authorities and thereby contributing to the avoidance of miscarriages of justice and to the fulfilment of the aims of Article 6. (See the following judgments of the Court: *Funke v. France*, 25 February 1993, Series A no. 256-A, p. 22, § 44; *John Murray v. the United Kingdom*, 8 February 1996, Reports of Judgments and Decisions 1996-I, p. 49, § 45; and *Saunders v. the United Kingdom*, 17 December 1996, Reports 1996-VI, p. 2064, § 68; *Serves v. France*, 20 October, 1997, Reports 1997-VI). The burden of proof cannot be reversed for the suspect to provide the requested evidence or prove his/her innocence.

Paragraph 7.10 – International Issues

This is a surprising and foolish attempt to deceive the UK public. In fact the OECD guidelines on cryptography are a minor part of the international effort to co-ordinate encryption policy. In particular the UK Government subscribes to the Wassenaar Arrangement, a major international activity that is being used to restrict the availability of strong encryption products, even those intended for civil use. (See the Cyber-Rights & Cyber-Liberties (UK) report, "Wassenaar Controls, Cyber-Crime and Information Terrorism", September 1998, at http://www.cyber-rights.org/crypto/wassenaar.htm)

The reasons for omitting any mention of the Wassenaar Arrangement are fairly easy to see. This agreement is quite explicit in stating that it should not be used to impede genuine civil transactions. However, despite this clear constraint, the UK Government has been misusing this agreement to justify restrictions on cryptographic products intended for civil use.

This activity by the US, the UK and other Governments has a major impact on the development of e-commerce because it seriously restricts the availability of the encryption products on which e-commerce depends.

The omission of any discussion of the impact of the Wassenaar Arrangement on the development of e-commerce could hardly have been an oversight since all the parties in the study team are very well aware of its existence and its impact. This can only be a reprehensible attempt to divert attention away from a key area where a policy change is needed but one in which the Government wants to avoid any discussion because its actions in the area are undermining rather than promoting the development of electronic commerce.