HC Trade and Industry Committee
Electronic Commerce Inquiry

Memorandum by
Cyber-Rights & Cyber-Liberties (UK)

February 1999

(1) Cyber-Rights & Cyber-Liberties (UK) (http://www.cyber-righs.org), which was founded in January 1997 with the aim of promoting free speech and privacy in regard to the Internet, welcomes the opportunity to make a written submission to the HC Trade and Industry Select Committee on Electronic Commerce Inquiry.

(2) This submission will concentrate on selected issues which reflect our current research into the protection of individual rights and liberties in the Information Age. Therefore we will not for example address "consumer protection issues" (which we have dealt elsewhere).[1]

(3) In this submission we will address one particular area which has been of great concern not only from a civil liberties perspective but also from a legal perspective - the problems of the Internet for law enforcement authorities. Therefore, this submission will deal with law enforcement issues in relation to

- the use of strong encryption,
- the desire of the law enforcement agencies such as NCIS to access "private encryption keys", and
- the issues surrounding police access to personal information through Internet Service Providers, including the activities of the ACPO/ISPs Government Forum.

---

[1] See for example Cyber-Rights & Cyber-Liberties (UK) Report: "Who Watches the Watchmen: Part II - Accountability & Effective Self-Regulation in the Information Age," September 1998 at http://www.cyber-rights.org/watchmen-ii.htm

(4) Law enforcement issues are expected to be dealt by the Government in its proposed Secure Electronic Commerce Bill as announced in the Queen's Speech last year, but the Bill has not yet been published.

Part A: Issues associated with key escrow, law enforcement and privacy concerns.

(5) **The issue of Privacy and the DTI's Approach** - A survey of recent Internet-related papers issued by the DTI would strongly suggest that privacy is not one of its prime concerns. So far, privacy issues in relation to the use of strong encryption systems have never been discussed or addressed by the DTI. This silence is especially remarkable in the light of other governmental initiatives. A right to privacy will soon be part of our lives within the United Kingdom under the Human Rights Act 1998 and a "right to respect for private life" will become part of the British law for the first time by reference to article 8 of the European Convention on Human Rights and Fundamental Freedoms (1950):

> "(1) Everyone has the right to respect for his private and family life, his home and his correspondence
>
> (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder of crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

It will be noted that Article 8 expressly incorporates a right to privacy in "correspondence", and this has long been interpreted by the European Court of Human Rights as including privacy in relation to communications via telecommunications networks. Indeed, the United Kingdom has already been found to be in breach of article 8 on several occasions for failing to pay adequate attention to the value of privacy.[2] We feel that there is a substantial risk that Internet-related proposals emanating from the DTI are in danger of repeating this error.

(6) Furthermore, principle 5 of the OECD Guidelines on Cryptography Policy stated that "the fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods." In addition to the OECD Guidelines, the European Commission's Communication on Encryption and Electronic Signatures points out that:

> "International treaties, constitutions and laws guarantee the fundamental right to privacy including secrecy of communications (Art. 12 Universal Declaration of

---

[2] See *Malone v. U.K.* App no. 8691/79, Ser. A. vol. 82, (1984) 7 EHRR 14; *Govell v United Kingdom* App.no. 27237/95 [1997] EHRLR 438; *Halford v UK*, App. no. 20605/92, 1997-III, (1997) 24 EHRR 523.

> Human Rights, Art. 17 International Covenant on Civil and Political Rights, Art. 8 European Convention on Human Rights, Art. F(2) Treaty on EU, EU Data Protection Directive)…….. Therefore, the debate about the prohibition or limitation of the use of encryption directly affects the right to privacy, its effective exercise and the harmonisation of data protection laws in the Internal Market."[3]

(7) These national and international developments, which express significant support for data privacy, should have important implications for the treatment of encryption. The use of encryption should be *prima facie* respected and even encouraged. By contrast, the government approach should be criticised as being fixated on the value of encryption solely in connection with commerce and ignoring wider political and social uses of information technology which might legitimately require the use of encryption.

(8) Law Enforcement and Encryption - To date, crime prevention has been the major published reason behind the official drive towards access to private encryption keys by the law enforcement agencies. Most people would accept the need for democratic governments to intercept communications on a limited scale, for detection and investigation of crime, and for the "defence of the realm". However, we will show in our evidence that the benefits of using strong encryption are far more important than the assumption that it might create problems for law enforcement.

(9) Ministers are aware of the benefits of using encryption technology for the development of e-commerce and for establishing business confidence in the Information Age, so there is no need to repeat them here.

(10) However, law enforcement agencies have tempered this enthusiasm for encryption with the fear that it might become a mechanism used by criminals and to protect evidence of criminality. First, the US FBI insisted on access to encryption keys and on a key escrow (or key recovery) mechanism for protection against terrorism, violent crime, foreign threats, drug trafficking, espionage, kidnapping, and other crimes. NCIS took a similar position in January 1999.[4]

(11) Without the "key recovery" capability, such law enforcement agencies contend that they would be less able to protect the safety of the public, and this in itself would constitute an infringement of civil liberties. However, we believe that the solution to the problems of crime prevention and law enforcement do not lie with accessing private encryption keys. From our own research into recorded criminal uses of encryption, we have concluded that

---

3 European Commission Communication, "Towards A European Framework for Digital Signatures And Encryption," Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions ensuring Security and Trust in Electronic Communication, COM (97) 503, October 1997, at <http://www.ispo.cec.be/eif/policy/97503toc.html>.

4 National Criminal Intelligence Service Press Release, NCIS calls upon Government to ensure law enforcement powers do not fall behind technology in fight against "crypto criminals" No: 02/99, January 26, 1999.

the use of encryption has not been a serious problem for crime detection or prevention. There is no more than speculation that it will be a problem in the future. In any event, it seems fanciful to expect that criminals will use government-mandated encryption systems with key recovery capabilities when alternative systems of encryption remain readily available. Government strategy would be naive if it assumed that criminals would use encryption tools which can be decrypted by the law enforcement bodies. In discussion, some Government spokesmen accept that criminals will communicate with one another securely outside any key escrow scheme. The point they make is that criminals communicating with innocent third parties who participate in a key escrow scheme will thereby expose those communications to interception. Innocent third parties are of course normally willing to assist law enforcement authorities by providing information, although in some cases they will rightly insist on police obtaining proper legal authority (the banks are the obvious example). If the police can obtain the information from innocent third parties by consent or through legal warrant, why do they need key escrow? We perceive that there are two possible reasons.

- The first is that key escrow outflanks the need to obtain proper legal authority for the disclosures. That is of course not an acceptable justification for key escrow, and is, on the contrary, a basic objection to it. The absence of proper legal authority and proper legal oversight will undoubtedly result in contraventions of article 8 of the European Convention.[5]
- The second is that key escrow provides the information "in real time", without the delay of approaching the innocent recipient, and also without the risk that that approach will reveal to the subject of investigation that the information has been obtained. It may be that there is genuine evidence from unreported investigations that real obstacles are being placed in the way of the detection and prevention of serious crime by the fact that information can only be obtained after a delay and with some risk of "tipping off". But it is striking that neither Government nor law enforcement spokesmen have ever clearly addressed this supposed problem, and have provided no evidence whatever in support of the only legitimate case that could support key escrow proposals. That case, if ever made, must take account of the fact, as pointed out by the European Commission, that "restricting the use of encryption could well prevent law-abiding companies and citizens from protecting themselves against criminal attacks. It would not however prevent totally criminals from using these technologies."[6]

Moreover, a key escrow technology will have a chilling effect on the on-line users who seek to remain either secure or anonymous when communicating through the Internet, whether for fear of retribution or other reasons.

---

5 See further *Klass v Germany*; Judgement of 6 September 1978, A.28; (1979) 2EHRR 214; *Huvig v France*, (1990) 12 EHRR 547.

6 See the European Commission, "Towards A European Framework for Digital Signatures And Encryption," Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions ensuring Security and Trust in Electronic Communication, October 1997, COM (97) 503, at <http://www.ispo.cec.be/eif/policy/97503toc.html>

(12) Denning and Baugh state that encryption is used by organised crime and for espionage and they cite seven cases of terrorism which involved encrypted files within computers, but in all of these cases the law enforcement agents managed to decrypt the files during their investigation.[7] Examples cited by the NCIS 26 January, 1999 press release are also weak evidence of law enforcement difficulties because they all involved cases in which law enforcement was successful in one way or another. Even without a "key escrow" or "key recovery" system, the law enforcement agents managed to decrypt the encrypted files in these cases. A case that is not mentioned by NCIS is the case of *Father Adrian McLeish*, a Roman Catholic priest, who was sentenced to six years' imprisonment in November 1996 for child abuse and child pornography offences.[8] During Operation Modem by the Durham Police, it was discovered that McLeish used encryption software. But McLeish's use of encryption was not a problem for the Durham police, as McLeish handed over his encryption keys together with his private passphrase - "Overhead the moon is beaming".[9]

(13) There are also practical issues here which are worthy of consideration. Of course we are not in favour of terrorists and drug dealers using cryptography to plan or facilitate their crimes. But what if they do? The sending of messages in this way may still create evidence which is obtainable during the course of an investigation or trial. It is suspect users who should be targeted, not the whole world at large. We should also remember that government access to encryption keys, just as the use of other technological surveillance (such as Closed Circuit Television systems ("CCTVs") or explosives detection equipment and X-ray machines) have not prevented premeditated brutal terrorist attacks such as the Lockerbie Pan AM 103 bombing, and the London Docklands, and Manchester Arndale shopping centre bombings. It takes an extraordinarily high level of constant surveillance and oversight to provide an effective deterrent through these means.

(14) More likely is that the terrorists will use encryption without detection or detection will come later through other means, by which time the refusal to provide the key will be incriminating evidence.[10] Terrorists and organised criminals are detected through a variety of techniques involving mainly informers and surveillance. The interception of messages is important, but the police clearly have powers effective to build up other useful evidence.

---

7 See Denning, D. E. &. Baugh, Jr., W. E, "Cases Involving Encryption in Crime and Terrorism," October 1997, <http://guru.cosc.georgetown.edu/~denning/crypto/cases.html>. Dorothy E. Denning is Professor, Computer Science Department, Georgetown University, Washington, USA, and William E. Baugh, Jr. is Vice President, Information and Technology Systems Sector, Science Applications International Corporation.

8 McLeish admitted 12 specimen charges of indecent assaults against two boys of 10, one aged 12 and another aged 18. He also admitted distributing indecent photographs, possessing them with intent to distribute them and being involved in the importation of pornographic videos of children.

9 Another example is the use of encryption within the so called W0nderland child pornography club with codes from the former Soviet KGB to prevent outsiders from gaining access to them. However, during the "Operation Cathedral" in September 1998, the misuse of encryption technology proved not to be a problem for the law enforcement forces around the globe for the detection of their criminal activity.

10 As under the Prevention of Terrorism (Temporary Provisions) Act 1989 sched.7.

(15) The March 1997 DTI Consultation paper suggested that similar legislation to the Interception of Communications Act 1985 will be introduced for the recovery of keys from the TTPs. Similar calls are now being made by NCIS in addition to the DTI proposals. But this idea seems to go further than the requirements of the 1985 Act because the consultation paper suggested that the future legislation will not only deal with information on the move through a telecommunications system but also for "lawful access to data stored and encrypted by the clients of the licensed TTPs". Additionally, Internet communications are different from simple telephone communications, and the encryption technology in question is obviously not the medium itself, but a tool that can be used for many purposes. So the analogy with the Interception of Communications Act 1985 is not necessarily a correct one.

(16) In developing its policy on encryption, the April 1998 Government *Secure Electronic Statement* relates that it has given serious consideration to the risk that criminals and terrorists will exploit strong encryption techniques to protect their activities from detection by law enforcement agencies. Therefore the government favours judicial warrants and legal interception of communications on a case by case basis. The policy paper stated that "the new powers will apply to those holding such information (whether licensed or not) and to users of encryption products." This is justified by the fact that warrants are regularly used for the interception of communications within Britain, although there is no claim that the interception of encrypted messages through the use of the Internet arose in any single case out of the 2600 interception warrants issued during 1996-97 by the Home Secretary. Another important issue to be noted is that the number of such warrants has risen considerably in the last few years (1073 warrants issued in 1996 compared to 473 in 1990).[11] This suggests both that the current powers are more than adequate and perhaps also that they are not being properly or strictly regulated.

(17) A further point which causes some alarm is that the government is not wholly committed to searches purely under the authority of a judge (contrary to earlier promises). In the *Secure Electronic Statement*, a vague distinction is made between judicial involvement in "criminal investigations" and other "interceptions" which will be by order of the Secretary of State. To some extent, it must be admitted that this follows the lax pattern of earlier legislation,[12] but the replication of this absence of proper (judicial) oversight should hardly be welcome. The effect will be to dilute considerably judicial oversight, as law enforcement agencies will be encouraged to engage in "fishing expeditions" for intelligence which do not require scrutiny by judges. In any event, the access to a key in order to decode a message already sent should be treated as a different exercise to the original interception of a message as it is being transmitted. Once an encrypted message has been intercepted and found undecipherable, the benefits of real time access have already been

---

11 Total figures for warrants issued in England and Wales 1989-1995: 1989- 458, 1990 - 515, 1991 - 732, 1992 - 874, 1993 - 998, 1994 - 947, 1995 - 997, 1996 - 1073. 'UK: Phone-tapping doubles in 5 years', Statewatch Bulletin, Vol 6 no 3, May-June 1996, and also the Report of the Commissioner for 1996, Interception of Communications Act 1985. Cm 3678, HMSO; Report of the Commissioner for 1996, Security Service Act 1989, Cm 3679, HMSO; Report of the Commissioner for 1996, Intelligence Services Act 1994, . Cm 3677, HMSO.

12 Compare the Interception of Communications Act 1985 with the Police Act 1997 Part III.

lost, and the process of enforcing access becomes analogous to executing a search warrant. That analogy should be applied, thus ensuring that access powers are subject to judicial authority and that the additional protection provided by the Police and Criminal Evidence Act for "special procedure materials", such as legally privileged communications, are properly respected.

(18) Alternative forms of evidence-gathering - The interception of messages is an important technique of modern law enforcement, but it should be remembered that terrorists and organised criminals are detected through a variety of techniques involving mainly informers and surveillance. It should also be remembered that encryption is a means to an end and that at some stage a decrypted message is quite likely to be produced and recorded on computer or even in physical form by the criminal. In addition, those who choose to exercise their "right to silence" by not disclosing information to unlock encrypted files will risk adverse inferences being drawn from their silence under sections 34-37 of the Criminal Justice and Public Order Act 1994. Lord Slynn in *Murray v. DPP* stated that:[13]

"If aspects of the evidence taken alone or in combination with other facts clearly call for an explanation which the accused ought to be in a position to give, if an explanation exists, then a failure to give any explanation may as a matter of common sense allow the drawing of an inference that there is no explanation and that the accused is guilty."

Not providing an encryption key may result in judges commenting on the accused's behaviour and juries drawing inferences under the 1994 Act. An even more draconian power to order an explanation of seized materials (such as a computer disk) exists under Schedule 7 paragraph 6 of the Prevention of Terrorism (Temporary Provisions) Act 1989.

(19) Conclusion - The EU communication paper on encryption stated that "most of the (few) criminal cases involving encryption that are quoted as examples for the need of regulation concern 'professional' use of encryption. It seems unlikely that in such cases the use of encryption could be effectively controlled by regulation."[14]

Part B: Issues associated with police access to personal information through the ISPs

(20) The Interception of Communications Act 1985 was enacted in reaction to the unregulated usage of interception of telephone conversations following the European Court of Human Rights decision in *Malone* v. *United Kingdom*.[15] It must be noted that although

---

13 97 Cr. App. R. 151 at 160.

14 European Commission Communication, "Towards A European Framework for Digital Signatures And Encryption," Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions ensuring Security and Trust in Electronic Communication, COM (97) 503, October 1997, at <http://www.ispo.cec.be/eif/policy/97503toc.html>.

15 *Malone v. U.K.* App no. 8691/79, Ser. A. vol. 82, (1984) 7 EHRR 14.

access to the content of communications has now been regulated, information about those communications derived from traffic logs remains unregulated.[16] A sophisticated electronic telecommunications system could provide a significant volume of information about who called whom when, which would in turn enable dossiers to be compiled showing the existence of networks of relationships between subscribers, without any requirement for a warrant. We believe, the whole system needs statutory revision and judicial control in order to comply with the European Convention on Human Rights.[17]

(21) A further point to be noted is that the interception regime applies to licensed providers of public telecommunications systems, and that very few Internet Service Providers ("ISPs") fall into this category. They are neither proper addressees of a 1985 Act warrant from the Secretary of State, nor beneficiaries of the protection given by the imposition of criminal sanctions against unauthorised interception. This limitation suggests that consideration be given to legislation which allows ISP to be notified as third parties to a warrant application. In any event, as in Germany and in several other Western European countries, we suggest that the objects of the investigation be informed of the issuance of a warrant at the end of its period of operation or such date thereafter determined by a judge on proof that earlier disclosure would hinder an ongoing investigation. Without such notification and possible scrutiny by an outside person, there is a grave danger that they system will be abused and that the European Convention standards will not be met.

(22) As became clear from the decision of the House of Lords in *R* v. *Preston*,[18] the statutory provisions for maintaining the secrecy of the fact of interception, and the narrowly expressed purpose of the power itself, have led to difficulties in the use of intercepted evidence: all material must be destroyed as soon as its retention is no longer necessary for the prevention or detection of crime, which must usually be inconsistent with its retention for use in a prosecution. The secrecy of the process, and the vesting of the relevant power in the Executive rather than the Judiciary, have effectively prevented the development of a body of case law bearing on the substance of interception issues. Therefore, a further reform may be a needed in the form of the abolition of section 9 of the Interception of Communications Act 1985 as supported by the Lloyd Report on Terrorism Legislation in 1996.[19]

(23) Internet Service Providers thus find themselves operating in an uneasy territory, subject to powers of search, perhaps exposed to criticism as holders (albeit unknowingly) of material used for criminal purposes, unable to be given the cover of a warrant from the Secretary of State for disclosing information, and in possession of information about the source and destination of messages which the authorities can obtain freely from telecommunications operators but which the very operations of an ISP render inaccessible without interception of the messages themselves.

---

16 See Schedule 2 of the Interception of Communications Act 1985.

17 This view is more fully expressed by JUSTICE, *Surveillanc*e (London, 1998).

18 [1994] 2 A.C. 130, H.L.

19 See Inquiry into Legislation against Terrorism (Cm.3420, 1996) (*the Lloyd Report*).

(24) Given the concern over cyber-crimes it is entirely understandable that the police and the ISPs should wish to develop mutual understanding and support, and to establish working relationships. For this purpose the Association of Chief Police Officers and the ISPs, with the support of the Home Office, have established the "ACPO, ISPs and the Government Forum." with the objective of developing good practice guidelines between Law Enforcement Agencies and the Internet Service Providers Industry, describing what information can lawfully and reasonably be provided to Law Enforcement Agencies, and the procedures to be followed. This initiative has caused considerable and legitimate concern among the British Internet users and the media.

(25) To date the work of the Forum seems to have been focused on developing and harmonising a form of request for information by the police to an ISP. The form, which might seem to some addressees to have the appearance of a legal warrant (akin to a search warrant), is designed to satisfy the ISP that in the circumstances of the particular case the ISP is not prevented by the restrictions on data disclosure in the Data Protection Act 1984 from providing information to the police. Despite its appearance, the form (and its associated "good practice guidelines") has no legal basis for imposing any obligation on an ISP to provide any form of disclosure to the police. In reality it is an invitation to volunteer information.

(26) It is of course right that the police should not put ISPs in peril of infringing the Data Protection Act, and to that extent the use of such a form is of assistance to all concerned. But it is most unfortunate that the Forum should so completely neglect the matter of the protection granted by the law to the safeguarding of private information, especially in the light of Article 8 of the European Convention.

(27) It may be argued that the investigation of crime excuses breaches of confidence, or negates the confidentiality itself. It is certainly a truism that there is no confidence in iniquity. This is an over-simplified view of the matter, however. It has certainly never prevailed over the need for judicial authority for disclosures by banks, and there is no reason why ISPs should stand in any different position.

(28) Furthermore there are important cases where the rule does not apply at all: communications protected by legal professional privilege (and lawyers are among those making increasing use of the Internet for professional purposes) remain protected however gross the iniquities revealed by them may be. And it is thoroughly unsatisfactory to expect ISPs to examine material sought by the police in order to determine, at their own expense, on their own responsibility and at their own risk, whether the degree of iniquity revealed justifies what would otherwise be a breach of confidence.

(29) As a result of concerns expressed about these issues, Cyber-Rights & Cyber-Liberties (UK) has developed a "privacy letter"[20] to be sent from a subscriber to an ISP addressing the position from the subscriber's point of view. A few ISPs have already replied as they are

[20] See the Cyber-Rights & Cyber-Liberties (UK) privacy letter at <http://www.cyber-rights.org/privacy/letter.htm>.

responsive to these concerns, but further evidence is needed before conclusions can be drawn.

(30) So far, the views of civil liberties organisations and, more importantly, the views of the users have been excluded from the ACPO ISP Government Forum: no doubt it is partly as a result of this exclusion that the Forum's initiatives and work, if unchecked, could lead to extensive infringements of the privacy rights of individual Internet users in the UK.

(31) Our recent report ("Who Watches the Watchmen: Part III - ISP Capabilities for the Provision of Personal Information to the Police," February 1999, at http://www.cyber-rights.org/privacy/watchmen-iii.htm) shows that we, together with the online users, have legitimate concerns in relation to privacy issues involving the Internet Service Providers and law enforcement bodies. Furthermore, procedures can only be properly designed within a legal context, and we are concerned to ensure that the legal context takes due account of individual rights and liberties. Such procedures are a matter of legitimate public interest, especially to users of the services of ISPs.

(32) It should be noted that the Association of Chief Police Officers has no statutory basis. Therefore, ACPO has no accountability to the public at large. Moreover, ISPA a trade body interested in protecting its own interests rather than the consumer interests, is also not accountable to the public. It is the duty of the Government to take such decisions and to open the closed doors to the public. Transparency, openness and accountability are important features of a healthy society and the Nolan Committee principles on good standards in public life should be respected. Policing the Internet by consent means winning the consent of the Internet user community: it cannot be achieved by recruiting Internet Service Providers as a private police force.

(33)We believe it is now time for the Government through Parliament to intervene in the activities of the ACPO/ISPs, Government Forum and clarify these matters, including the laws in relation to interception of communications and the relevant procedures. We believe this should be a heavily regulated area otherwise we can expect several detrimental consequences, including further litigation under the European Convention/Human Rights Act and a transfer of business to legal jurisdictions which better respect the value of privacy.

The Cyber-Rights & Cyber-Liberties (UK) Memorandum has been written by:

Mr. Yaman Akdeniz, Director;
Professor Clive Walker, Deputy Director;
Mr Nicholas Bohm, E-Commerce Policy Adviser