CABINET
OFFICE

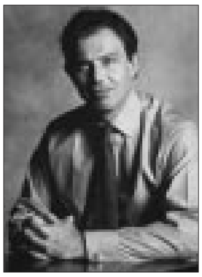
performance and innovation unit

Encryption and Law Enforcement

A PERFORMANCE AND INNOVATION UNIT REPORT – MAY 1999 performance and innovation unit

FOREWORD

BY THE PRIME MINISTER



I am determined to ensure that the UK provides the best environment in the world for electronic business. Only by taking a lead to promote electronic business will we reap the potential economic and social benefits. But I am equally determined to ensure that the UK remains a safe and free country in which to live and work.

The rise of encryption technologies threatens to bring the achievement of these two objectives into conflict. On the one hand, business has delivered a clear message that encryption is essential for developing confidence in the security of electronic transactions. And lack of confidence is often cited as one of the main brakes on electronic commerce. People also want to enhance the security of their personal communications through the use of encryption. To meet these needs, the Government is keen to support the strong and growing market in encryption products and services.

On the other hand, the use of encryption by major criminals and terrorists could seriously frustrate the work of the law enforcement agencies. Indeed there is already evidence that criminals, such as paedophiles and terrorists, are using encryption to conceal their activities. It is a little known fact that on average one in every two interception warrants issued results in the arrest of a person involved in serious crime. If powers of interception and seizure are rendered ineffective by encryption, all society will suffer. So it is vital that in our support for the use of encryption we limit the damage to our ability to protect society.

In February 1999, I asked the Performance and Innovation Unit (PIU) to consider the issue of encryption, e-commerce and law enforcement and a task force was established to look quickly at the problem. This report draws on the findings of this PIU task force and on the work of the Unit's wider e-commerce project. It sets out the issues surrounding encryption and law enforcement and the encryption task force's recommendations to achieve better-balanced Government policy in this area.

I see this report as a way of securing greater public understanding of some of the issues at stake. The value of interception as a law enforcement tool is one such issue. Clearly, sensitive operational techniques need to be protected because of national security concerns. But this report sets out as fully as possible the findings of the PIU task force in demonstrating the Government's intention to encourage a public debate.

I particularly welcome their recommendations for moves towards closer co-operation between Government and industry to ensure that together we achieve our twin aims: a continued safe society for all – and the best environment in the world for electronic business.

Tony Blair

Tony Blair

CONTENTS

ANNEXES

Encryption and Law Enforcement

1. Summary

Developments in encryption technology, products and services carry significant benefits in increasing consumers' levels of trust in the Internet, and particularly in e-commerce. However, they also give rise to a number of challenges for law enforcement, where it will become more difficult to derive intelligence from lawfully intercepted communications and retrieved data. This report considers the Government's response to the issues of encryption, e-commerce and law enforcement. The report is framed by two key objectives for the Government:

- to make the UK the best environment in the world in which to trade electronically; and
- to ensure that the UK remains a safe country in which to live and work.

The task force concluded that no single technique or system was likely to be enough to sustain law enforcement capabilities in the face of rising use of encryption by criminals. This being the case, a package of measures was needed to mitigate the consequences as set out below.

Recommendations

- The voluntary licensing of providers of encryption services, proposed in the recent DTI consultation document on the forthcoming Electronic Commerce Bill, will help improve consumers' confidence and therefore support the development of e-commerce in the UK. However, these licensed providers should *not* be required to retain 'decryption keys' or to deposit them with third parties (i.e. no mandatory 'key escrow'). Whilst the introduction of a mandatory link between licensed providers of services and key escrow would provide the best technical solution to many of the problems caused by encryption, in practice it would not support achievement of both of the Government's objectives.
- The Government should adopt a new approach based on co-operation with industry to balance the aim of giving the UK the world's best environment for e-commerce with the needs of law enforcement. There is no 'silver bullet' policy that guarantees that the development of encryption will not affect law enforcement capabilities.
- A new Government/industry joint forum should be established to discuss the development of encryption technologies and to ensure that the needs of law enforcement agencies are taken into account by the market. This new co-operation should also be promoted at the international level. The forum should consist of a high-level group to discuss policy issues and be supported by specialist technical and legal groups.

- A new Technical Assistance Centre should be established, operating on a 24-hour basis, to help law enforcement agencies derive intelligence from lawfully intercepted encrypted communications and lawfully retrieved stored data. The Technical Assistance Centre will also be responsible for gaining access to decryption keys, where they exist, under proper authorisation.
- The task force welcomes the intention to include in the forthcoming Electronic Commerce Bill provisions to allow lawful access to decryption keys and/or plain text under proper authority. The task force also recommended that further attention should be given in the Bill to placing the onus on the recipient of a disclosure notice to prove to the authorities that the requested keys or plain text are not in his possession, and to state to the best of his knowledge and belief where they are.
- The UK should encourage the development of an international framework, including a new forum, to deal with the impact of encryption on law enforcement.

Topics covered in this section:

- *Remit of the PIU study*
- *Methodology*

2. INTRODUCTION

Remit of the PIU study

2.1 The creation of the Performance and Innovation Unit (PIU) was announced by the Prime Minister on 28 July 1998. Its aims are to improve the capacity of government to address strategic, cross-cutting issues and promote innovation in the development of policy and delivery of the Government's objectives. The PIU acts as a resource for the whole of government, tackling issues on a project basis. Annex A provides more information on the role of the PIU.

2.2 In February 1999 the Prime Minister asked the PIU to consider the issue of encryption and law enforcement. The PIU was already conducting a project to examine how the Government's objective of making the UK the world's best environment for electronic commerce would most effectively be achieved (as announced by the Prime Minister in December 1998). It then became clear that more detailed work was needed on whether and how to regulate the use of encryption in the DTI's Electronic Commerce Bill.

2.3 The remit given to the PIU was:

- to study the needs of law enforcement agencies and of business;
- to examine the merits of the current encryption policy (and in particular key escrow, which is explained in chapter 5); and, if necessary,
- to identify proposals that would satisfy both the need to promote encryption for electronic commerce and the Government's duty to ensure that public safety is not jeopardised.

Methodology

2.4 To handle this remit, the PIU established a joint Government/industry task force to examine the issue and to recommend a way forward. The task force was led by David Hendon, Chief Executive of the Radiocommunications Agency, and worked alongside the existing PIU electronic commerce project team, led by Jim Norton. Its membership was drawn from:

- the Home Office;
- the National Criminal Intelligence Service;
- GCHQ Communications-Electronics Security Group;
- the Department of Trade and Industry;
- the Cabinet Office;
- British Telecommunications; and
- IBM.

2.5 The PIU task force had a very short time to complete its work and was tasked with identifying the broad strategy rather than the detail of implementation. Over the six-week period of its creation and work, the task force had discussions with 23 companies and organisations and with five overseas governments. The task force reported to the Prime Minister at the end of March 1999. This report draws on the findings of the task force and on the work of the PIU's wider e-commerce project. It sets out the issues surrounding encryption and law enforcement and the encryption task force's recommendations to achieve better-balanced Government policy in this area.

Topics covered in this section:

- *Government policy on e-commerce*
- *The importance of encryption to e-commerce*

3. DEVELOPING ELECTRONIC COMMERCE IN THE UK AND THE ROLE OF ENCRYPTION

GOVERNMENT POLICY ON E-COMMERCE

3.1 The Government is committed to promoting electronic commerce in the UK. The cost savings available from streamlining business processes and supply chains using e-commerce techniques are dramatic: reduced time to market, lower stock holdings, reduced transaction costs. All these offer substantial benefits to industry and consumer alike. Entirely new ways of doing business are also enabled, such as holding electronic auctions for airline tickets or hotel rooms. The pace of development around the world is unprecedented, but much depends on ensuring trust in this new medium and here encryption technologies have a vital role to play.

3.2 The Government's broad electronic commerce agenda was published in October 1998 in *Net Benefit: the electronic commerce agenda for the UK.*[1] Further to this, in the White Paper *Our Competitive Future: Building the Knowledge-Driven Economy,*[2] published in December 1998, the Government set out the ambitious goal of developing the UK as the world's best environment for electronic trading by 2002. The PIU's electronic commerce project team has been tasked to identify the strategy necessary to meet this objective and is due to report by Summer 1999.

3.3 The DTI continues to work actively in this area, driving forward competition, meeting with the e-commerce supply sectors to tackle barriers to growth, and helping small businesses take full advantage of the explosion of new ways to access, use and send information. The Government's commitment to e-commerce in its widest sense was further spelled out in the March 1999 White Paper *Modernising Government*. Chapter 5 of the White Paper makes it clear that the Government will use new technology to help meet the needs of citizens and business in the provision of public services, and not trail behind technological developments.

THE IMPORTANCE OF ENCRYPTION TO E-COMMERCE

3.4 Encryption can be used to provide a variety of security services for commercial transactions. Principally these are integrity, authentication and confidentiality. Integrity services can guarantee that data has not been accidentally or deliberately corrupted; authentication guarantees that the originator or recipient of material is the person they claim to be; and confidentiality ensures that data cannot be read by anyone other than the intended recipients.

3.5 All of these services are important to overcome the lack of trust felt by many people in the security of information sent over the Internet. This lack of trust is often cited as one of the most significant barriers to the increased use of electronic commerce.

3.6 Encryption can be used by business, for example, to guarantee:

- that contracts have not been improperly altered, and have been signed by authorised personnel;
- that funds are transferred securely, by replacing information like credit card

[1] URN 98/895
[2] CM 4176

details or account numbers in such a way that they cannot be used fraudulently; and

- that market sensitive information flowing between different parts of an organisation cannot be accessed by anyone other than those entitled to see it.

3.7 Encryption also has benefits in helping to protect the privacy of personal communications. Whether individuals are corresponding with friends using e-mail, or electronically booking appointments with their doctor, some people will wish for the added security that comes from using encryption.

A FAMILIAR USE OF ENCRYPTION IN THE HOME

One familiar commercial use of encryption is to prevent free reception of satellite TV. Without advanced encryption devices, programmes delivered into homes could be viewed by anyone. Encryption allows only the person who has paid to view the programmes to watch them. The technology also makes it virtually impossible to tamper with a decoder to extract and copy the key, which is supplied over the air.

A BUSINESS USE OF ENCRYPTION

The world-wide Automotive Network Exchange (ANX) is a system being developed collectively by vehicle manufacturers. It is a private network using Internet technologies (an Extranet). The network binds together manufacturers, contractors, sub-contractors and component suppliers throughout the industry supply chain. Through this network flow computer-aided design information and manufacturing files, purchase orders, shipment details, electronic payments and a wide variety of other business information. Encryption technology is used in a variety of ways:

- integrity services assure that order information has not been corrupted;
- authentication services assure that orders and invoices are genuine; and
- confidentiality services protect proprietary design information.

Encryption continues to make a significant contribution to areas such as the 72% reduction in error rates experienced since the introduction of ANX.

Topics covered in this section:

- *The importance of interception for effective law enforcement*
- *Government policy on interception*
- *The impact on interception of developing encryption technologies*
- *A shared international problem*

4. LAW ENFORCEMENT ISSUES RAISED BY ENCRYPTION

4.1 The development of encryption technology gives rise to a number of challenges to law enforcement, security and intelligence agencies. In particular, its widespread use will have an effect on the ability of these agencies to make use of lawfully intercepted communications and retrieved data for law enforcement purposes. This chapter assesses the importance of interception for law enforcement and considers the impact of encryption on law enforcement capabilities.

The importance of interception for effective law enforcement

4.2 It is sometimes claimed that interception has rarely led to the successful prosecution of a criminal and that equally good intelligence can be gained by other means. This is simply untrue. Interception of communications has long been an essential tool in the fight against serious crime and threats to national security. It is long-standing policy not to disclose details of interception operations so as not to undermine its value as an intelligence source. But the following figures give an idea of the value of the existing arrangements. During 1996 and 1997, lawful interception of communications played a part – often the crucial part – in operations by police and HM Customs which led to:

- 1,200 arrests;
- the seizure of nearly 3 tonnes of class A drugs;
- the seizure of 112 tonnes of other drugs with a combined street value of over £600 million; and
- the seizure of over 450 firearms.

4.3 During this period, around 2,600 interception warrants were issued by the Home Secretary. This means that on average one person involved in serious crime was arrested for every two warrants issued.

4.4 In addition to being highly effective, interception also gives many advantages over other investigative methods, such as surveillance and the use of informants. Surveillance is extremely expensive in its use of resources compared with interception. To work successfully it must be targeted very carefully, usually in conjunction with some other form of intelligence gathering mechanism such as interception. The use of informants often fails to give the direct and unbiased access which can be gained by interception. Informants are not always available, cannot always be relied upon and seldom offer the kind of direct coverage provided by interception. In many investigations, interception may be the only possible means of access to a target who is alert to surveillance and against whom no informants can be recruited.

4.5 The task force noted that there is a general public acceptance of the use of telephone and mail interception under warrant with the aim of protecting society. Yet there appears to be a very strong aversion in some quarters to law enforcement agencies having similar warranted access to the electronic communications that are the common currency of the Internet community. The task force therefore felt it important to emphasise to this community the importance of lawful interception in protecting society from crime and terrorism. They believed it was important 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.

EXAMPLES OF ENCRYPTION USED IN SERIOUS CRIME

- In 1995 two suspected paedophiles were arrested by police in the UK on suspicion of distributing child pornography on the Internet. Their computer systems were found to contain pornographic images of children and, in the case of the leading suspect, a large amount of encrypted material. The indications were that the suspects had used encrypted communications to distribute child pornography to contacts around the world via e-mail. Although both paedophiles were subsequently convicted of distributing child pornography, the police investigation into the leading suspect was severely hampered by the fact that he had used encryption.
- In late 1996, a police operation culminated in the arrests of several leading members of a Northern Irish terrorist group and the seizure of computer equipment containing encrypted files. The files held information on potential terrorist targets such as police officers and politicians. The data was eventually retrieved but only after considerable effort.
- In 1998, police enquiries into a case of attempted murder and sexual assault were impeded by the discovery of encrypted material on a suspect's computer. The investigation was able to proceed only after the relevant decryption key was discovered by the police amongst other material seized from the suspect.

Government policy on interception

4.6 Under the Interception of Communications Act (IOCA) 1985, interception of any communication (including e-mail) on a public telecommunications network requires a warrant to be signed by a Secretary of State. Interception may only be authorised where the Secretary of State considers that it is necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or for the purpose of safeguarding the economic well-being of the United Kingdom. IOCA requires the Secretary of State to consider, before authorising an interception, whether the information could reasonably be obtained by any other (less intrusive) method. An independent Commissioner keeps under review the exercise of the Secretary of State's powers under the Act. The Commissioner submits an annual report to the Prime Minister who lays it before Parliament.
It is open to anyone who believes that his or her communications may have been intercepted to apply to the Interception Tribunal established under IOCA which investigates complaints.

4.7 The proposals contained in this report are, therefore, not about increasing the scope of interception, or access to stored data. They are designed to ensure that lawfully intercepted and retrieved material can continue to provide intelligence to the law enforcement agencies in order to assist the investigation of serious crimes and terrorism.

4.8 The PIU task force suggested that the law enforcement agencies should adopt a more pro-active approach to making people aware of the value of interception in the fight against serious crime, to the extent possible whilst not compromising the technique's effectiveness.

The impact on interception of developing encryption technologies

4.9 The widespread deployment of encryption means that it will become increasingly difficult for law enforcement agencies to make use of communications when they are lawfully intercepted.

4.10 The problem is urgent. There is a general acceptance that encryption will become a more generic technology, and thus integrated into an ever larger number of applications and products. For example, there are indications that some Internet Service Providers in the UK will make strong encryption tools available on their introductory CDs, giving many Internet subscribers the opportunity, at little cost to themselves, to use strong encryption techniques for both their stored and communicated data. The advent of Internet telephony and of encrypted mobile phones also has the potential to reduce the information that can be derived by law enforcement agencies from interception under warrant.

INTERNET TELEPHONY

Voice and data are increasingly converging onto a single, Internet Protocol (IP) based, transport network. Currently, telephone calls use the (circuit-switched) Public Switched Telephone Network – where a path is opened across the network between the calling parties for the duration of the call. In an IP communication, on the other hand, the call is divided up into many small packets, which are sent individually by any number of different routes and reassembled at the other end. Both circuit-switched telephony and IP data are conveyed in a digital form, and digitisation of the network has allowed telecommunications operators to offer many new services to users. A technology known as ’Voice Over IP’ is increasingly being suggested as a replacement for Public Switched Telephone Network voice calls, as rationalisation of switching methods leads to savings for operators. Technical change in telecommunications is further accelerated by new service providers entering the market and improving competition. Operators wishing to attract new customers, or to earn additional revenue from existing customers, are increasingly likely to offer encryption services as value-added services, especially as encryption is more readily applied to digital rather than the older analogue transmissions.

4.11 Much of the encryption used when communicating or storing data will be effectively unbreakable by the authorities. For example, readily available strong encryption technology means that many billions of different combinations potentially need to be tried before a code can be broken. The time and computer resources needed to do this make the code unbreakable in a reasonable time. For most police operations, information is needed as soon as possible; most encryption would take far too long to crack for the decoded information still to be of use. A fuller account of the requirements for law enforcement when dealing with encrypted material is at Annex B.

CODE BREAKING (‘BRUTE-FORCE ATTACKS’)

How easy is it to crack an encrypted message? Digital encryption keys are classified according to how may ’bits’ they have. To take the example of a readily available 128-bit key; using a ’brute force’ approach – with a billion computers that are able to try a billion keys per second (which is far beyond anything available at present) – it would still take the decrypter 10,000,000,000,000 years to try all of the possible combinations. That is something like a thousand times the age of the universe.

A SHARED INTERNATIONAL PROBLEM

4.12 Whilst the study has largely concentrated on the domestic scene, the PIU task force also took account of the views and experiences of the Governments of the USA, Canada, Sweden, France and Germany. It is clear that law enforcement agencies in all these countries, and many others, are facing similar problems. Although the degree of lost lawful interception currently caused by the use of encryption in different countries is variable, there is a general expectation that the problem posed by encryption for law enforcement can only get worse. All the countries with which this issue was raised expressed a desire to co-operate with other governments and with industry to tackle the impact of encryption on law enforcement.

Topics covered in this section:

- *Public Key Cryptography*
- *Digital signatures*
- *Key escrow and licensing*

5. GOVERNMENT CONSIDERATION OF ENCRYPTION POLICY

5.1 In chapter 3, the importance of encryption to the development of electronic commerce, as a means of guaranteeing integrity, authentication and confidentiality, was demonstrated. Chapter 4 assessed the impact of encryption on law enforcement capabilities and, in particular, on the ability of law enforcement agencies to derive intelligence from seized and intercepted material. Taken together, these two preceding chapters make clear that there is a balance to be struck between the needs of business and law enforcement. This chapter goes on to set out the Government's recent approach to regulating providers of encryption services with the aim of striking that balance. It also considers the likely way in which encryption services will be provided to customers across the Internet, specifically explaining the structure of Public Key Cryptography, as the most likely form of service provision.

Public Key Cryptography

5.2 The widespread use of cryptography has only become feasible because of the invention of what has become known as Public Key Cryptography. In such a system, users' keys come in pairs, known as public and private keys. As the names suggest, the private keys are only known to their owners, whereas public keys can be made available to anyone. A private key cannot be derived from the corresponding public key.

5.3 Messages can now be enciphered using the intended recipient's public key. The private key needed to decipher the message is known only to the recipient. Therefore, only the recipient can decipher the message content. It is obviously important for the sender of the message not only to be able to gain access to the recipient's public key, but also to be confident that it does indeed pertain to the correct and intended recipient. Public keys are very often made accessible to all; they are bound to the identity of their individual owner by 'wrapping' them in a digital certificate, signed by a recognised and trusted Certification Authority (CA). This important supporting infrastructure is commonly known as a Public Key Infrastructure (PKI).

ENCRYPTED MESSAGES AND PUBLIC KEY INFRASTRUCTURE

This example illustrates data confidentiality. The same PKI can be used to support secure electronic signatures. Different keys are typically used for the different services.

If two people, A and B, want to send each other encrypted messages:

1. A arranges to have a key pair certificated by the Certification Authority providing the Public Key Infrastructure service. A must prove his identity to the Certification Authority who then vouches for the fact that A indeed has the private key corresponding to the certificated public key.
2. A keeps the private key securely, whilst the public key is published complete with its certificate attached.
3. B uses A's public key to encrypt his message, having first verified for authenticity the associated certificate for A.
4. B then sends the encrypted message to A (in some cases enclosing his own public key where this is necessary).
5. A uses his private key (and if necessary B's public key) to decode the message.

Note: In key escrow both A and B's private data encryption keys (but not their signature keys) would be stored (escrowed) with a Trust Service Provider.

Digital signatures

5.4 Public Key Cryptography can also be used to guarantee the integrity and authenticity of data, whether the data itself is to be enciphered or not. (The signing of a bank cheque is often regarded as a helpful analogy.) With encryption, this is done by a process that combines use of a private signature key with the data that is to be signed to construct a (message dependent) digital signature. This signature can be validated with knowledge only of the associated public key. Hence anyone can be confident that the owner of the key pair constructed both the signature and the data to which that particular signature is attached.

5.5 Again, for this to work it is essential for verifiers of the signature to be confident that the relevant key pair is properly identified to its real owner. So in these circumstances access to the public key would normally be achieved via a digital certificate, itself signed by a trusted CA. Attaching such a digital signature to an electronic document has significant benefits for engendering trust in electronic commerce. When they receive a document with such a signature, a recipient will know that the document has genuinely come from the claimed originator. Digital signatures have the potential to open up new areas of business to electronic commerce, for example by making a reality of electronic signing of contracts.

5.6 Digital signatures do not pose the same problem to law enforcement. They could even bring significant law enforcement benefits, as they would help an individual sender or recipient to be positively identified and may also help cut down on fraudulent transactions.

Key escrow and licensing

5.7 In 1996, the Government proposed that providers of data encryption and digital signature services should be obliged to apply for official licensing as 'Trusted Third Parties'. Such mandatory licensing would be designed to help establish the market by guaranteeing to consumers that certain standards were adhered to by the service providers. For law enforcement purposes, an important condition of the proposed licensing regime was that service providers would be required to keep copies of their customers' private data encryption keys (but not signature keys), so that, if required, law enforcement agencies could access them under warrant.

5.8 'Key escrow' is the arrangement whereby a copy of the key that enables the content of a document to be subsequently recovered is held securely by a third party. Licensed key escrow refers to a system where a copy of the key is held by a trusted third party, who has satisfied the stringent regulations concerning maintenance and custody of client keys, generally – but not always – the company that is providing the encryption service.

5.9 Industry's response to these proposals included a concern that mandatory licensing for encryption service providers would slow the take-up of electronic commerce. It was also argued that criminals would avoid the controls by making their own arrangements, while British business and commerce would be competitively disadvantaged by having to build their e-commerce systems in the particular way that the Government required.

5.10 In April 1998, the Government decided that policy should be relaxed. Instead of mandatory licensing for encryption and digital signature service providers, it proposed that licensing would be voluntary. However, the requirement to operate data encryption key escrow remained for those companies that wished to exploit the cachet of being licensed.

5.11 Digital signatures supported by providers who met the regulatory requirements were thought likely to carry a greater legal presumption of authenticity than those issued by unlicensed providers. This would be an encouragement for people to use licensed providers. Companies hoping to avoid key escrow would not be allowed to gain the benefits of licensing for operating just a signature service. The proposal was that there should be an 'all or nothing' approach, i.e. companies licensed to provide digital signatures that also wished to provide encryption services could only do so under licence.

5.12 Government trailed a change to this policy, in the DTI's latest consultation document on the Electronic Commerce Bill, *Building Confidence in Electronic Commerce*, issued on 5 March 1999. This consulted on the basis that key escrow or third party key recovery would not be a requirement for licensing, and that licensing itself would in any case be voluntary.

Topics covered in this section:

- *The merits of key escrow*
- *The limitations of key escrow*
- *Conclusions on key escrow*

6. ANALYSIS OF KEY ESCROW

6.1 As stated above, the PIU task force was to examine the merits of the originally proposed linkage between licensing and key escrow. This chapter assesses the merits and limitations of key escrow, from the perspective of industry and consumers. It also considers the extent to which key escrow, or other forms of third party key recovery, would address the law enforcement concerns raised by encryption.

The merits of key escrow

6.2 For business and consumers, a system of Government-licensed providers of encryption services, together with licensed Trust Service Providers holding copies of encryption keys, carries a number of potential benefits:

- the licensing of Trust Service Providers would provide reassurance to users that their confidentiality requirements are being met by a company that meets certain minimum standards of service provision (analogous to a British Standard kite mark);
- a properly implemented and managed third party key recovery system would help increase users' confidence that their keys are properly maintained and access to them is given only to those having a proper, lawful permission; and
- a Key escrow (or key recovery) system would permit the retrieval of important data by users themselves, for example if confidentiality keys were accidentally lost or perhaps destroyed by a departing or disaffected employee.

6.3 In terms of law enforcement requirements, the merits of key escrow would to some extent depend on the ease with which it could be avoided, nationally or internationally. This is considered further below. However, if key escrow was widely adopted and implemented, then the task force concluded that, in terms of the public policy response to developing encryption technologies, no other technique would give anything like the same functionality in meeting the needs of law enforcement in their task of ensuring the UK is a safe place in which to live and work.

6.4 Having obtained the particular 'key warrant', in addition to the authority to intercept the communications of a suspected serious criminal, key escrow would allow the police and law enforcement agencies to decrypt such communications cheaply and easily, thereby retaining similar levels of intelligence to those they currently have. Seized encrypted material might be similarly examined.

6.5 The obvious question is why criminals would use a key escrow system which made keys available to the police and other law enforcement agencies. The PIU task force took the view that this is not a persuasive argument against key escrow, concluding that:

- criminals generally use technology that is readily available. Indeed, criminals continue to use landline telephones, even though it is well known that their communications can be intercepted; and
- criminals have to deal with legitimate businesses including travel agents, car hire companies and others who will not be interested in evading normal commercial arrangements.

The task force did, however, recognise and agree with the Government's previous assessment that a proportion of more sophisticated criminals would be unlikely to use any Government-sanctioned encryption system.

The limitations of key escrow

6.6 The task force's in-depth interviews with industry highlighted a number of critical concerns about key escrow. These can be divided as follows:

- concerns as to the viability of key escrow as a technique in providing electronic confidentiality products and services. As there is no large-scale working model of an escrowed Public Key Infrastructure, these concerns as to scalability and security cannot be resolved at present;
- commercial problems affecting the extent to which market forces could be expected to drive key escrow as an industry standard;
- difficulties arising from the global nature of e-commerce which would interact with these technical and commercial problems if the UK adopted a stand-alone key escrow policy.

6.7 These issues are explored further in the boxes below.

STATED TECHNICAL OBJECTIONS TO KEY ESCROW

- An escrowed Public Key Infrastructure may not scale to millions of users because of its inherent complexity; it is untried technology.
- A 'key store' would represent a single concentration of vulnerability, which may be subject to sophisticated attack by hackers. However, an advantage is that this risk is more easily addressed by implementing strong security at a single location.
- Adoption of key escrow could cut UK industry off from the mainstream development of new encryption protocols, with consequential cost and functionality limitations.
- Some technologies make use of a new key for each message (known as 'session keys'). Because of the potential number of them, these keys are not suited to storage.

COMMERCIAL CONCERNS WITH KEY ESCROW

Companies interviewed by the task force raised the following problems with key escrow:

- Key escrow is perceived as adding costs to a Public Key Infrastructure supporting public confidentiality services;
- potential UK Trust Service Providers would be reluctant to be licensed under a regime that mandated key escrow as a condition of licensing;
- Key escrow could be expected to involve some additional capital and running costs that would have to be passed on to customers; and
- it would be difficult to react quickly to the changing Internet business environment if it was also necessary to meet the UK's unique escrow requirements.

For key escrow to be successful in meeting the law enforcement requirements, it would need to become the industry standard and 'blue chip' service providers would need to lead the way in marketing licensed services. The lack of commercial enthusiasm to be licensed represents a major hurdle which would need to be overcome.

DIFFICULTIES WITH KEY ESCROW ARISING FROM THE GLOBAL NATURE OF E-COMMERCE

The task force considered that the range of technical and commercial objections to key escrow were such that adoption of key escrow would be unlikely to take place solely through the action of market forces – it could only be driven by legislation. Domestic legislation in the UK alone would raise further difficulties:

- the Internet does not respect national boundaries. A potential user of encryption services would be able to choose from all those offered commercially, regardless of where they originated;
- it is probable that UK users would opt for simpler, cheaper encryption services located outside the UK if key escrow imposed additional costs on domestic providers;
- a market might well develop outside the UK for services that offered themselves as 'defending the individual's right to privacy' by avoiding key escrow; and

continued >

- on the basis of discussions with other countries, and in particular with EU member states, there would be a danger of driving the UK's encryption market overseas if key escrow was implemented in the UK alone. UK firms would, of course, be free to market their services back into the UK from any EU country.

These concerns suggest that a stand-alone UK regulatory framework for encryption would be unlikely to be effective.

Conclusions on key escrow

6.8 In the abstract, key escrow and other forms of third-party key recovery have a number of attractions as a public policy response in meeting the concerns of law enforcement in the face of developing encryption technologies. However, a system of key escrow with Trusted Third Parties could only be effective if it was widely adopted in the UK and international marketplace.

6.9 In assessing likely domestic and international developments in encryption, the task force concluded that:

- widespread adoption of key escrow was unlikely in the current industry and public climate. It was evident that the opportunity to put in place a single Public Key Infrastructure incorporating key escrow had passed. Many different products and services are already being introduced into a market that is changing rapidly;
- the proposed voluntary licensing of providers of electronic encryption services would help improve consumers' confidence and would therefore support the development of e-commerce in the UK;
- implementation of mandatory key escrow would significantly impair the ability of the UK to become the leading environment in the world in which to trade electronically. It would be shunned by UK business which has to compete in world markets and against competitors established in other countries; and
- in the light of the above, key escrow as a condition of licensing would not deliver to law enforcement agencies even a reasonable amount of assured access to decrypted communications.

6.10 The PIU task force therefore recommended that the Government should reform policy so that licensed providers should not be required to deposit data encryption keys with third parties (i.e. no mandatory 'key escrow'). The introduction of a mandatory link between licensed providers of services and key escrow would not support the Government's twin objectives on e-commerce and law enforcement.

Topics covered in this section:

- *A new Government/industry joint forum*
- *Establishment of a Technical Assistance Centre*
- *Legislative issues*
- *International issues*

7. A NEW APPROACH

7.1 In the absence of key escrow, the task force recommended that the Government should adopt a new approach based on co-operation with industry to balance the aim of giving the UK the world's best environment for e-commerce with the needs of law enforcement. The task force identified no 'silver bullet' policy that would guarantee that the development of encryption did not affect the capability of law enforcement to derive intelligence from intercepted communications. In future, a package of measures will be needed in developing a credible strategy to limit the harm done by encryption and to maintain public safety. The main elements of this strategy are recommended below.

A new Government/industry joint forum

7.2 The PIU task force found that, to some extent, the development of a more credible strategy had been hampered by poor Government/industry co-operation. In large part the debate has focused on key escrow to the detriment of everything else. And yet co-operation between Government and industry is vital to:

- help industry understand the threats to law enforcement from emerging technologies;
- enable law enforcement to understand market trends and realities; and
- allow Government and business to work together in order to achieve a workable balance between commercial and law enforcement interests, leading to the adoption of appropriate practices and standards in the provision of Internet and telecommunications services.

7.3 This co-operation would need to be based on trust between the parties. The task force hoped that this will be helped by the unambiguous statement that key escrow is not to be an element of the licensing regime, reflecting the concerns of industry. Greater co-operation would also expose business to the important public safety interests at stake.

7.4 As a focus for this new co-operative approach, the PIU task force recommended the establishment of a joint Government/industry forum. This idea was warmly welcomed by the companies the task force spoke to. The forum would include the Cabinet Office's Central IT Unit, representing government as a purchaser and user of IT products and services.

7.5 The forum might have a high-level policy group with a subordinate specialist technical and legal structure. The purpose of the forum will be to ensure that industry is consulted on, and given a structured opportunity to contribute positively to, Government policy in this area. The chairman of the high-level policy group should be a senior official from the Department of Trade and Industry. When established, this co-operation should be promoted internationally. It is proposed that the forum should be assisted by the establishment of an encryption co-ordination unit within the Home Office. This unit will provide assistance on matters connected with policy, technology and standards, and act as a secretariat and as a focal point for international liaison.

Establishment of a Technical Assistance Centre

7.6 There is currently no dedicated resource to assist law enforcement agencies with accessing plain communications or text from encrypted material. The PIU task force therefore recommended the establishment of an operational Technical Assistance Centre in secure premises, operating on a 24 hour basis. This would, where possible, carry out decryption of lawfully intercepted or recovered material not supplied in plain-text format, seeking assistance from industry where necessary. Such decryption would involve the routine application of appropriate methodologies, where the keys are available. It would provide a means of rapid consultation with industry where access to plain text is hindered by the need to identify the communications or storage protocol structures.

Legislative issues

7.7 The task force found that current legislation is inadequate to deal with the challenges for law enforcement that are likely to arise as a result of the increasing use of encryption. In this respect, the task force welcomes the intention to include in the Electronic Commerce Bill provisions to allow lawful access to decryption keys and/or plain text under proper authority. The task force also recommended that further attention should be given in the Bill to placing the onus on the recipient of a disclosure notice to prove to the authorities that the requested keys or plain text are not in his possession, and to state to the best of his knowledge and belief where they are.

7.8 During the course of the study, the task force found that industry shares many of the concerns of Government with respect to the misuse of encryption for criminal purposes. For business, this is particularly relevant to cases of fraud and intellectual property theft. In this respect, the view of some of the countries and organisations consulted was that it should be made a criminal offence to use encryption in the furtherance of a crime. In other words there would be a penalty (of a nature to be determined) if encryption for confidentiality was used by an individual or a body in either planning or carrying out a crime. The task force considered the option of such an approach, but concluded that this should not be pursued. It was unlikely to be of any practical benefit in deterring the criminal use of encryption and risked being seen as criminalising the use of encryption.

7.9 The task force noted that a review of the Interception of Communications Act 1985 was under way within the Home Office. It was recognised that the findings of this review would have an important read-across to the Government's policy on encryption.

International issues

7.10 The task force considered that as encryption, like electronic commerce, is a world-wide phenomenon, there must be a greater degree of international co-operation – particularly in relation to setting agreed standards. To be effective, solutions concerning the regulation or use of encryption must be made to work internationally. However, apart from the OECD Guidelines on Cryptography Policy,[3] there has been remarkably little co-ordination of policy on encryption matters. The result has been a degree of misunderstanding and suspicion as to the rationale behind attempts to regulate, or influence, the domestic use of encryption. The real case for law enforcement has not been made effectively.

7.11 The task force considered that efforts should be made to ensure that the law enforcement requirement is recognised and accepted by international policy and standardisation bodies. This will involve sustained international co-operation between HMG and other governments to promote law enforcement access as a legitimate regulatory requirement. There is therefore a potential need for a new international framework for dealing with this issue. Following discussions with the leading countries on encryption matters, the PIU task force recommended that the Government should continue discussions with foreign governments with a view to seeking support for a new forum to promote co-operation on policy, law enforcement, and technical and standards matters relating to encryption.

[3] The Guidelines on Cryptography Policy were drawn up in 1996 and published in March 1997 by the OECD.

ANNEX A:
ROLE OF THE PERFORMANCE AND INNOVATION UNIT

The creation of the Performance and Innovation Unit (PIU) was announced by the Prime Minister on 28 July 1998 as part of the changes following a review of the effectiveness of the centre of government by Sir Richard Wilson. The PIU's aim is to improve the capacity of government to address strategic, cross-cutting issues and promote innovation in the development of policy and in the delivery of the Government's objectives. The PIU is part of the drive for better, more joined-up government. It acts as a resource for the whole of government, tackling issues that cross public sector institutional boundaries on a project basis.

The Unit reports direct to the Prime Minister through Sir Richard Wilson and is headed by a Senior Civil Servant, Mr Suma Chakrabarti. It has a small central team that helps recommend project subjects, manages the Unit's work and follows up projects' recommendations with departments. Work on the projects themselves is carried out by small teams assembled both from inside and outside government. About half of the current project team staff are drawn from outside Whitehall, including from private sector consultancies, academia and local government.

The first set of PIU projects were announced by the Prime Minister in December 1998. The aim is to complete most of them by late summer/autumn 1999. The projects are:

- Developing Electronic Commerce in the UK – how to make the UK the world's best environment for electronic commerce, ensuring that the UK benefits fully from the single fastest growing marketplace in the global economy;
- Active Ageing – how to improve the well-being and quality of life of older people by helping them to remain active. The study will identify ways of increasing the employment opportunities for older people, by examining the incentives for businesses to employ and retain older people and for individuals to remain in paid or voluntary work;
- Central Government's Role at Regional & Local Level – getting the right institutional arrangements and relationships in place for joined-up delivery of central Government policies in regions and communities;
- Accountability and Incentives for Joined-Up Government – examining how current accountability arrangements and incentive systems can be reformed to facilitate joined-up policy-making and delivery, for example by promoting achievement of joint objectives which require co-operation between departments; and
- Objectives for Rural Economies – examining the differing needs of local rural economies, and the key factors affecting performance, so as to establish clear objectives for Government policies influencing the future development of rural economies.

The Unit is also separately identifying the key future challenges that government will have to face, as referred to in the Government's *Modernising Government* White Paper, published in April 1999. This work will help departments and other organisations to look beyond their existing policies towards the Government's long-term goals.

ANNEX B:
LAW ENFORCEMENT REQUIREMENTS

INTERCEPTION OF ENCRYPTED COMMUNICATIONS

The following represent law enforcement's ideal requirements in order to maintain the effectiveness of interception in the face of criminal use of encryption:

- to be effective, interception must take place without the knowledge of either party to the communication. Therefore, decryption must also take place without either party being aware that it is happening;
- one of the most useful features of interception is that it enables information to be gathered in 'real time' (as it happens). Decryption of communications must take place as close as possible to real time to maintain the effectiveness of the power;
- there needs to be a means of identifying the sender and recipient of a message and the identity of the key holder; and
- law enforcement agencies require sufficient information in order to decrypt intercepted communications to and from a target. In general this will mean the provision of keys necessary for decryption. The provision of plain text may be acceptable if it is provided in such a way as to ensure that only the law enforcement agency is aware of the content (to protect the target's right to privacy and operational security) and it is accompanied by sufficient information to ensure that the plain text provided is the original content of the communication.

ACCESS TO ENCRYPTED STORED DATA

Similarly, a number of factors applying to lawful access to stored data must also be applied to lawful access to encrypted stored data, as follows:

- stored data must be retrieved in such a way as to ensure that its provenance can be proved in court, and handled in such a way as to maintain the 'chain of evidence'. Decryption of stored data must therefore take place in accordance with best practice on computer forensic evidence. In general, this may require access to the decryption key rather than the plain text (otherwise doubt might be cast in court on the authenticity of the plain text); and
- access to the stored data must be within a legal time limit imposed by the instrument under which it is obtained (e.g. a production order issued by a court might require compliance within five working days). Decryption must therefore be able to take place within the same timescale as the statutory power.

DELIVERY OF ENCRYPTED DATA TO WHICH LAWFUL ACCESS IS GIVEN

Any data lawfully intercepted or retrieved, or requests for such data, must be passed securely between the agency which has been given legitimate access and the Trust Service Provider, or other party providing access. Delivery must be effected in such a way that the data cannot be read or retrieved by anyone not having lawful access. This will protect both operational sensitivities and the privacy of users of encryption.

COST-EFFECTIVENESS

The current interception of communications regime is a cost-effective use of law enforcement resources. Ideally this would remain the case under a system that includes the decryption of lawfully intercepted communications.

Performance and Innovation Unit**, Horse Guards Road, London SW1P 3AL Published: May 1999 CABI J99-4278/9905/D16**