BILETA

16th BILETA Annual Conference

April 9th - 10th, 2001.
University of Edinburgh, Scotland.

Encryption, and the Regulation of Investigatory Powers Act 2000.

CLIVE WALKER
(University of Leeds, UK)

Encryption and the impact on rights

In common with the modes of communication they succeed and to some extent supplant, the new information technologies such as the Internet entail both positive and negative consequences for individual rights.

Amongst the negative impacts might be the ability to gather and transfer data concerning subjects in ways which at best commodify the personality of the individual and at worst facilitate unaccountable and even mistaken interferences with autonomy. These concerns are reflected in data protection laws which, more so in Europe than the USA, restrict the free market in data use for the sake of subject privacy, based around article 8. It will be noted that Article 8 expressly incorporates a right to privacy in regard to "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 this aspect of privacy.

More positively from the point of view of privacy interests, the technological mode of delivery of Internet communications can be utilised to afford effective protection for communications, especially through the use of strong encryption tools. Encryption may offer various advantages to the users of information technology.

- First, encryption can provide confidentiality and integrity for the information transferred from A to B. It can for example provide a secret transmission of content, ensuring that the message's integrity has not been overseen.
- Furthermore, with the use of encryption technology, B can authenticate that the information was sent by A. Digital signatures can be created by the use of encryption and these can authenticate the sender of the information as they cannot be forged.

All these points may be important for different reasons for the transmission of data over the Internet. Many are connected with business transactions and the desire to keep financial information away from the prying eyes of third parties who might then use the intercepted information for fraudulent purposes. In this way, encryption technology is a fundamental element for the development of a global electronic commercial system.

Other personal purposes of encryption include being able to obtain advice or counselling in private and perhaps even without identification.

Next, the same encryption technology can be used for securing true private communications

concerning public affairs. It has enabled the use of the Internet as a mode of information gathering and dissemination concerning, for example, human rights abuses.

Encryption Policy in Europe

In response to the needs for establishing trust and confidence through the use of encryption technology in the Information Age, there is a need for a regulatory framework at both national, supranational, and international level. However, far from having a consensus, there are considerable differences between the various regulatory framework initiatives offered by the European Union and in the USA. Furthermore, there are even completely different policy initiatives between the European Union member states. All these differences not only hamper and hold back the growth and development of e-commerce, but also the possibility of providing a trustworthy environment for netizens.

As early as 1994, the Bangemann Report to the European Commission dealt with the use of encryption tools and stated that a solution at a national (member states) level will inevitably prove to be insufficient because communications reach beyond national frontiers and because the principles of the internal market prohibit measures such as import bans on decoding equipment. Therefore, according to Bangemann a solution at the European level was needed "which provides a global answer to the problem of protection of encrypted signals and security.

In October 1997, the European Commission, published a communication paper, *Towards A European Framework for Digital Signatures And Encryption*. In contrast to some member states initiatives, the European Commission paper found key escrow and key recovery systems to be inefficient and ineffective and has sought to foster a permissive rather than restrictive regime. It has also reminded us that .

> "... 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."

The European Commission also dismissed the claims that the use of digital signatures would create problems for the law enforcement. For the purpose of creating a legal framework for the use of digital signatures, the European Commission, in May 1998, published a proposed Directive on a Common Framework for Electronic Signatures. The draft directive was finalised in October 1998 and highlighted the problem that "...different initiatives in the Member States lead to a divergent legal situation.... the relevant regulations, or the lack of them, will be different to the extent that the functioning of the Internal Market in the field of electronic signatures is going to be endangered." It warns against compulsory certification schemes, though there may be voluntary provision. The Directive was finalised in December 1999.

At the time of writing, the European Commission was yet to finalise a common policy on the use of encryption. This will be the more problematic task for the Commission as (again at the time of writing) for there are completely different policy views within the member states of the European Union.

These pro-encryption views are echoed in the OECD Guidelines on Cryptography Policy issued in 1997. These Guidelines are intended to promote electronic commerce, data security and privacy protection. Encryption plays a vital role, as is recognised by Principle 5 which states 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.". Likewise, the Council Of Europe concluded in 1999 that Internet users should be able to use all available means to protect communications, including encryption.

UK Encryption Policy: General

The UK government has been trying to formulate a policy on encryption since around 1994, but the many policy initiatives described below were complicated by having two different governments and by the need to take account of supranational (the European Union) and international (the OECD) policy initiatives on encryption.

At the outset, the UK's Department of Trade and Industry ("DTI") published a Paper, *On Regulatory Intent Concerning Use Of Encryption On Public Networks*, in June 1996 to meet the growing demands to safeguard the integrity and confidentiality of information sent electronically over the Internet. The UK Government proposed the introduction of the licensing of Trusted Third Parties ("TTPs") to hold the copies of all private encryption keys with the use of key recovery systems. This was followed by the Consultation Paper, *Licensing of Trusted Third Parties for the Provision of Encryption Services*, in March 1997.

Since the Labour Party had objected to key escrow while in opposition, it was expected that there would be a fresh look at encryption policy after the General Election in 1997. But a merely re-packaged version of policy was announced in spring 1998 by the Department of Trade and Industry under the title of *Secure Electronic Commerce Statement*. This not-so-new policy statement followed from the previous government's Trusted Third Party initiative, but this time the Trusted Service Providers (who must combine TTP and Certification Authority functions) could be employed by Internet users on a "voluntary basis", though those who do not use them could find certain presumptions of authenticity asserted against them. In addition, it remained a licensing condition for the TTPs to use key recovery systems favoured by the government.

The DTI's Statement was the inspiration behind the announcement within the Queen's Speech in November 1998 of proposed legislation in the form of a projected Electronic Commerce Bill. A consultation paper detailing the proposals was announced, and more details were given in a document issued in October 1998 by the DTI called, *Net Benefit: The Electronic Commerce Agenda for the UK*. The paper still contends that "encryption, has a major drawback - the same technology used to protect sensitive business communications can be used by criminals and terrorists to circumvent the legal powers of interception by governments." Therefore the Net Benefit paper states that:

> "In the UK, the Government is proposing to encourage the establishment of Trusted Third Parties (TTPs) where users of encryption keys could deposit their private encryption keys with licensed organisations which would provide legal access by law enforcement agencies. Introducing legislation to license such bodies will give both the public and business confidence that they are dealing with organisations providing professional key management and storage facilities."

A further DTI Consultation Paper, *Building Confidence in Electronic Commerce*, appeared in March 1999. The core strategy of key escrow and third party recovery and licensed Trust Service Providers, with OFTEL as the licensing authority, is again to the fore, though it remains in theory voluntary and more flexible licensing is envisaged in which key escrow is not a condition to obtain a licence. This all goes well beyond the relatively minor and technical legislative adjustments necessary to put electronic wiring and signatures on a par with physical versions.

Encryption policy was to be finalised in April 1999 in intensive discussions with the information technology industry following the publication of the consultation paper. Two developments halted the achievement of this goal.

- First, the meetings with industry sectors resulted in strong lobbying against many of the preferred solutions. The strong message came forward that they would be very damaging to e-

commerce and would therefore hinder the development of electronic trading.
- Secondly, the considerable delay also allowed agencies and groups championing civil liberties interests to gather their forces. They were encouraged to do by the House of Commons Select Committee on Trade and Industry, which decided in late 1998 to embark upon an inquiry into electronic commerce and published a critical report in 1999. It doubted whether there was a need for more than minimal technical legislation and rejected outright the official reliance upon enforcement of key escrow.

Mindful of this experience, the Cabinet Office's Performance and Innovation Unit's, *Encryption and Law Enforcement* (1999) emphasised that the way forward is for a "partnership" approach, with the partners being government and information technology industry.

Intended as the closure to the debate was the DTI Command Paper, *Promoting Electronic Commerce*, which incorporated draft legislation which has now become the Electronic Communications Act 2000. Significant shifts in regulatory policy included the shelving of plans for compulsory licensing of TSPs, to be replaced by a voluntary "approvals regime" in which the industry itself was to adopt self-regulatory kite-marking, but the threat of an imposed (and virtually unspecified) registration scheme for cryptography support services loom under Part I of the legislation if industry did not deliver.

This paper will now address specifically the issue of law enforcement and its balance with privacy rights.

UK Encryption Policy: Law Enforcement Concerns

Several deeply-seated factors have tended to impel policing agencies in late modern societies towards techniques of surveillance. One is that information technologies have developed enormously and pervade the economies and societies in western states. Their uses are both for good and ill, the latter being the subject of policing. At the same time, the technologies provide both a new site for policing activity and also furnish a variety of opportunities for surveillance which would not previously have been feasible. The trend next represents part of a fundamental switch away from the reactive policing of incidents to the proactive policing and management of risks. It follows that the interception of messages is an important technique of modern law enforcement. Accordingly, since the introduction of the White Paper in June 1996, a constant refrain from the government has been that encryption is a threat to criminal investigation and national security. It is feared that criminals and terrorists will exploit strong encryption techniques to protect their activities from detection by law enforcement agencies and that the law enforcement agencies such as NCIS will not be able to access "private encryption keys". 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 physically reproduced.

The original plans involved key escrow on a wide scale, so that the wider powers to intercept communications could bear fruit. However, later plans were slightly more modest and built upon established powers of interception or search. There are several objections to these plans.

- First, there is no proven need for any extension of interception powers in order to obtain deciphered messages. There is no evidence 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 and 1997 by the Home Secretary. These statistics are called in aid by the Cabinet Office's Performance and Innovation Unit paper (1999), which also mentions that the 2600 warrants resulted in 1200 arrests. These are also claimed to be reliable and cost effective, but not one is linked to the Internet or to encryption.

- *Second, the interception powers themselves are already out of constitutional control. The number of such warrants has risen alarmingly in the last few years. And there is no judicial oversight of the issuance of warrants which are on the authority of governmental ministers. The RIP Act Part I does not address these concerns, save that it provides for greater legality (but no greater scrutiny) in respect of the system of permissive disclosures on the request of a police inspector under the Data Protection Act 1998, section 29(3).

- In any event, the idea that TSPs will satisfy law enforcement concerns is far-fetched, and it is difficult to see any certain advantages. Such a structure can easily be evaded by criminals who can either take their business abroad or can simply use uncertified systems of encryption. Even after the vehement criticism of the Select Committee, still the Cabinet Office's Performance and Innovation Unit (1999) manages to see some merit in key escrow, believing that lazy criminal will use it by default or will be forced to do so by legitimate correspondents. However, the Cabinet Office does conclude that the balance of arguments has turned against key escrow because of uncertainty, costs and lack of global support.

An alternative to the discovery of the codes of keys from innocent (or unsuspecting) key holders is to demand the information from the suspect or even an innocent recipient. Already in law, those suspects 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 of the Criminal Justice and Public Order Act 1994. This form of erosion of due process rights was taken up by the DTI Consultation Paper, *Building Confidence in Electronic Commerce* which argued that there should be a new power to allow the police to require the disclosure of encryption keys on service of a written notice when encrypted data has been uncovered pursuant to existing search or intercept powers. It follows from that provenance that the written notice is not necessarily issued on the basis of judicial authority, but can be authorised by the Home Secretary as a follow up to an authorisation to intercept communications. The bones of the same idea were followed in the Cabinet Office paper and were given greater flesh in mid-1999 by the consultation paper, *Promoting Electronic Commerce*. and Part III of the draft Electronic Communications Bill. Part III proved to be the most contentious part of the draft Electronic Communications Bill and, to avoid undue delays, it was dropped from the proposals which have become the Electronic Communications Act 2000. At the same time, it was decided to combine the former Part III with other pending legislation which was to replace both IOCA and the ACPO Codes. The result is the Regulation of Investigatory Powers Act 2000, and Part III deals with encryption.

Section 49 grants the powers to require disclosure of any protected information where the authorities by notice to the person whom he believes to have possession of the encryption key, impose a disclosure requirement in respect of the protected information under section 49(2). Under section 49 (3), a disclosure requirement in respect of any protected information must be necessary:

> "(a) in the interests of national security;
>
> (b) for the purpose of preventing or detecting crime; or
>
> (c) in the interests of the economic well-being of the United Kingdom."

In the case of *Amann v. Switzerland*, the European Court of Human Rights stated that "tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated." This ruling, which condemned wording relating to national security, suggests that section 49(3) above is an inadequately detailed basis for disclosure powers.

Although section 49(9) states that a notice under this section shall not require the disclosure of any key which is intended to be used for the purpose only of generating electronic signatures, this intention of protecting the integrity of signature keys, will very often fail since RIPA also allows access to encryption keys. In many cryptographic products the same passphrase (or key) is used for both signature and confidentiality purposes, and this means that access to keys for protected information will also give access to signature keys. But this duality is confirmed in the draft Code of Practice.

Section 50 deals with the effect of notices imposing disclosure and requires the person who has been served a section 49 notice to convey the information in an intelligible form (under section 50(1)(b)). The provision of any private keys which are capable of decrypting the protected information would also suffice for complying with a section 49 notice under section 50(2)(a). However, under section 50(3), disclosure of any key to the protected information that is in the possession of the person who has been served a section 49 notice at a relevant time could be required if for example the notice states, in pursuance of a direction under section 51, that it can be complied with only by the disclosure of a key to the information as stated in section 50(3)(c). Many critics believe that any form of GAK is very damaging to trust and confidence in the use of public key cryptography. Accordingly, section 51 seeks to limit the situations in which direct access to keys can be required. Under section 51(4), a person shall not give a direction unless he believes:

> "(a) that there are special circumstances of the case which mean that the purposes for which it was believed necessary to impose the requirement in question would be defeated, in whole or in part, if the direction were not given; and
>
> (b) that the giving of the direction is proportionate to what is sought to be achieved by prohibiting any compliance with the requirement in question otherwise than by the disclosure of the key itself."

Under section 51(5), the matters to be taken into account in considering whether the requirement of subsection (4)(b) is satisfied in the case of any direction shall include the extent and nature of any protected information, in addition to the protected information in respect of which the disclosure requirement is imposed, to which the key is also a key. However, the scope of the phrase "special circumstances" in section 51(4)(a) is not legally defined.

Section 52 deals with payments for disclosure. It shall be the duty of the Secretary of State to ensure that appropriate arrangements are in force for requiring or authorising contributions towards the costs incurred by compliance with section 49 notices. Any disclosure will immediately result in the replacement of keys, so payments by the government are inevitable and could (if calculated at true cost) be substantial.

Section 53 deals with a failure to comply with a section 49 notice, A person to whom a section 49 notice has been given will be guilty of an offence (with a maximum penalty of two years' imprisonment) if he knowingly fails to make the disclosure required. Under section 53(2), in proceedings against any person for an offence under this section, if it is shown that that person was in possession of a key to any protected information at any time before the time of the giving of the section 49 notice, that person shall be taken for the purposes of those proceedings to have continued to be in possession of that key at all subsequent times, unless it is shown that the key was not in his possession after the giving of the notice and before the time by which he was required to disclose it. This places the burden of proof on defendants to show that they no longer hold a key that they may previously have held. The presumption of continued ownership is unfair (as contrary to rights concerning the burden of proof and rights against self incrimination under Article 6 of the Convention), since the burden should remain throughout on the prosecution to show that the accused is in a position to provide the key and deliberately refuses to do so. At least section 53 has improved dramatically since it was first introduced within the draft Electronic Communications Bill. In its

finalised form, under section 53(3), a person shall be taken to have shown that he was not in possession of a key to protected information at a particular time if:

> "(a) sufficient evidence of that fact is adduced to raise an issue with respect to it; and
>
> (b) the contrary is not proved beyond a reasonable doubt."

So the defendant does not have to meet a very heavy subsequent responsive burden. Nevertheless, other issues relevant to fairness, such as the seriousness of the crime, the access to legal advice and the availability of other evidence, remain less settled, despite their emphasis in European Convention jurisprudence.

The Government disputed any infringement of Article 6, arguing that the enforcement agencies would already have the encrypted information and all they need is the encryption key to make the message intelligible:

> "In our view, the correct analysis is that a key has an existence independent of the will of the subject. We believe that that was explicitly approved by the European Court in the leading case of *Saunders v. United Kingdom* in 1996. The court found that the right against self-incrimination does not extend to the use in criminal proceedings of material that may be obtained from the accused for the use of compulsory powers, but which has an existence independent of the will of the suspect; for example, documents recovered under a warrant."
>
> Lord Bassam, House of Lords Debates, vol.614 col.972, 28 June 2000.

Section 54(1) deals with the tipping-off offence (with a five year maximum penalty). A person served with a section 49 notice, or every other person who becomes aware of it or of its contents, is required to keep secret the giving of the notice, its contents and the things done in pursuance of it. A specific defence to the above tipping-off offence is provided in section 54(5) if it is shown that

> "(a) the disclosure was effected entirely by the operation of software designed to indicate when a key to protected information has ceased to be secure; and
>
> (b) that person could not reasonably have been expected to take steps, after being given the notice or (as the case may be) becoming aware of it or of its contents, to prevent the disclosure."

Moving from duties placed on the private possessors of the data to the duties placed on the investigative authorities, under section 55(2), it shall be the duty of each of the persons to whom this section applies to ensure:

> "(e) that... any key so disclosed is stored, for so long as it is retained, in a secure manner;
>
> (f) that all records of a key so disclosed (if not destroyed earlier) are destroyed as soon as the key is no longer needed for the purpose of enabling protected information to be put into an intelligible form."

Although the Government has accepted that RIPA should include a commitment to the protection of seized keys, there also needs to be a clear commitment to employ the best available methods for key protection. But no guidance either in RIPA or in the draft Code of Practice is given on the design, development, implementation and operation of the procedures, standards and technical mechanisms needed to provide protection for keys. The fallback is an action in negligence, and the government has agreed that "the duty imposed on public authorities to look after keys should be actionable.".

However, there are no criminal offences attached to disclosure of a citizen's data. The conclusions of the Trade and Industry Committee were that "the proposed code of practice may prove to be toothless" and "the impression is given by the legislation that infringements of the code of practice will go unpunished".

To sum up, three problems arise in connection with Part III.

European Convention: It is not made clear what suspicion or belief should be established or what other evidence be possessed, or what other avenues of investigation be available or not prior to the issuance of a notice. Nor is it made clear there should be legal advice. Accordingly, it is strongly possible that such a requirement could breach Article 6 of the European Convention by reversing the burden of proof, especially as a failure to comply will itself be an offence and not just a matter of evidence in the trial as a whole (Salabiaku v France (1988); Saunders v UK (1997); R v Home Secretary, ex p Kebilene, 1999). At very least, the triggering criteria for the issuance of a notice ought to be very carefully defined, especially as the onus will be on the recipient of the notice to prove no knowledge.

Conflict with the Information age especially policies regarding e-commerce: The RIP Act associates encryption with criminality. This paper has tried to show that national government access to encryption keys would undermine and hold back both the development of e-commerce and the political use of the Internet in pursuit of privacy and free expression rights. As stated by the HC Select Committee:

> "...UK electronic commerce policy was for so long entrapped in the blind alley of key escrow that fears have been expressed that UK's reputation as a competitive environment for electronic commerce is now severely damaged. "
>
> House of Commons Select Committee on Trade and Industry, 1999, para.116)

Technical challenges: There are other methods of hiding identities and information which will not be covered in this paper, including, steganography, remailers, account cloning, and spoofing.

Conclusion

The policy stances of states in the non-Anglo-American world, including the European Union and OECD policy statements as described above, look very different and the trend is towards greater liberalisation. In order to explain the remaining differences between those information societies like the US and UK which are favourably disposed towards regulation of encryption and those like the European Union (and even France) which are less so inclined, we offer the following explanations.

In the first place, UK/US official position is reflective of underlying geo-policies and tensions, in other words the dominance of a state security agenda on the part of executives whose world authority is in large part based on military might . Set in the context of the richest and most militarily powerful country in the world, the US concerns that the dissemination of encryption techniques will weaken this power seem strikingly implausible. There is no convincing evidence that the use of encryption has created significant new problems for defence or law enforcement interests in the US. The same seems to be true from our survey of relevant United Kingdom case-studies, many cited by the government as evidence of the contrary but which invariably resulted in detection and conviction. Though the perfect criminal could use encryption technology to make detection very difficult, just as the perfect criminal could use a fast car to make a speedy getaway or wear overalls and plastic gloves to avoid the deposit of DNA materials. In reality, criminals are rarely perfectly conscientious or error-free, and we value fast cars, overalls - and encryption - for purposes other than their possible criminal applications.

A second explanation is that the different approaches also reflect distinct cultural stances in regard to the value of privacy. The UK especially has had a tradition of being a privacy-free legal zone. The USA does recognise privacy at federal and state level, but even so, the protection is at best patchy and is heavily tempered by the dominant value of First Amendment free speech. In contrast, the more regulated and corporatist polities of Western Europe have long developed respect for privacy, and their lead in data protection laws are a prime indicator of the difference from the Anglo and especially the American position. Yet, these differences may now be diminishing. One the one hand, the UK has now enacted the Human Rights Act 1998 which will broadly give effect to a right to privacy under article 8 of the European Convention. On the other hand, with the Maastricht Treaty (1992) and the establishment of a Third Pillar competency including home affairs and justice, the European Union has been drawn into not only policing matters in relation to police cooperation on interception of communications, including encryption but also is alleged to be considering controversial plans (under the project title, ENFOPOL) for wide-ranging and coordinated electronic surveillance which seem at odds with its underlying respect for privacy.

Our third explanation is that the Anglo-American dalliance with encryption is also motivated by forms of moral and political entrepreneurship on the part of some of the policing and security organisations within those jurisdictions. As some forms of policing business diminish, whether through the end of the Cold War or through the endless incarceration of an ever-increasing proportion of the population, other forms of business will be sought. Set against recent falling crime rates, the invocation of the threat of boundless pornography, fraud and vile racism has proven a useful well for the enterprising police or security officer to found a new empire and to secure funding for it. In this way, the Internet provides a paradigm of a late modern sub-society, in which the traditional structures of class or other socio-political commonality are replaced by new élites whose privilege is measured in terms of knowledge and technological access. In this case, the self-selecting élite are the cyber-cops who seek to claim better insights into the threats of the Internet than are understood by its users themselves. To help them further, a national encryption resource unit, GTAC, has been established in the Security Service building, a location which should remind us of the political importance of this area of policing.

Fortunately, the underlying conditions of Internet governance are set firmly against eccentric national regulation, as this is a medium that demands interactive solutions both between state and state but also state and citizen. Yet, the law has failed to keep pace with the ever more sophisticated surveillance techniques available not just to eager law enforcement agencies but also to possibly unscrupulous private persons. RIPA falls far short of an effective Parliamentary response. The law still does not offer a single legal regulatory system, even though one was promised by the Home Office. And the law remains weak in terms of the imposition of regulation and the protection for rights in electronic communications.

BIBLIOGRAPHY

Further details and full references can be found in:

Akdeniz, Y., and Walker, C., "Whisper who dares" in Akdeniz, Y., Walker, C., and Wall, D., *The Internet, Law and Society* (Longmans, London, 2000)

Akdeniz, Y., Taylor, N., and Walker, C., "BigBrother.gov.uk: State surveillance in the age of information and rights" [2001] *Criminal Law Review* (forthcoming)