Secrecy and Signatures—Turning the Legal Spotlight on Encryption and Electronic Signatures

MARTIN HOGG*

Go back to the AHRB Centre's publication section.

INTRODUCTION:

Of the subjects covered in this book, that which is perhaps the most controversial at the present time is cryptography, the technology underpinning both encryption and electronic signatures.[1] The proposals for legislation in this area have generated interest from a wide variety of bodies. This may be seen from the disparate parties who participated in the British Governmental and parliamentary consultations on electronic commerce. [2]These included the Confederation of British Industry, commercial enterprises (such as British Telecommunications plc), the Internet Service Providers' Association, academics, the National Criminal Intelligence Service, and civil rights groups (such as Cyber-Rights and Cyber-Liberties (UK)).

The interest generated was the result of varying concerns, amongst them human rights, privacy and the prevention and detection of crime. It is principally the phenomenal rise in the use of cryptography for commercial reasons, however, which has prompted the need for a consideration of the legal regulation of electronic signatures and encryption.

The British Government has now enacted an Electronic Communications Act.[3] The Government have managed to stick closely to their timetable for the promulgation of this Act, despite the view expressed by several parties that matters were proceeding at an unseemly pace merely in order to coincide with the millennial date. The Act is in three parts, and addresses cryptography service providers (Part I), electronic signatures and certificates (Part II), and Telecommunications licences and other matters (Part III). The first two parts are of particular concern inin thisthis chapter and the relevant provisions of the Act are discussed below. Provisions concerning law enforcement access to encrypted material are included in separate legislation, the Regulation of Investigatory Powers Bill. [3a]

The following discussion is divided into four parts. In the first part, there will be an explanation of the nature of cryptography, and the dependent applications of document encryption and electronic signatures; secondly, the current state of the law regarding these areas will be assessed; thirdly, proposals for law reform will be considered; and lastly, the international dimension, in so far as not already covered, will be considered.

CRYPTOGRAPHY, ENCRYPTION, AND ELECTRONIC SIGNATURES

Cryptography

In the business world, there has been an ever increasing interest in ensuring that electronic communications are afforded the qualities of authenticity, integrity and confidentiality. A handwritten signature has traditionally been the best guarantee of the first two of these qualities in a document: it uniquely verifies the person from whom the document originates,[4] and indicates assent to the contents of the text appearing above it.[5] Confidentiality has had to be assured by, or instance, enclosing the document in a sealed envelope. However, forgery is not unknown and envelopes can be opened and resealed. Technological developmentsnow offer a more iron cast guarantee of achieving all of these qualities,via the use of cryptography.

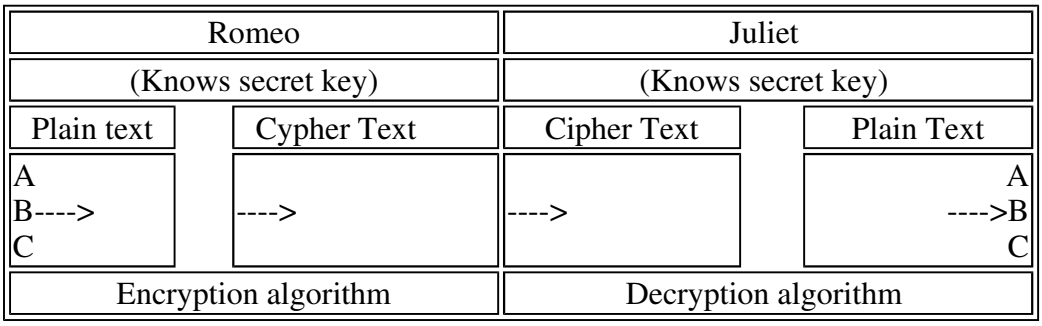
Cryptography is used to create electronic signatures (which are used toachieve authenticity and integrity) and to encrypt such signatures or other data (such as e-mails or commercial documents, thus achieving the end of confidentiality). Attempts to alter electronic signatures are easily detectable and the document's authenticity would then be doubted; attempts to decrypt an encrypted document should prove impossible if a secure enough encryption program has been used. If company A wishes to send company B a confidential electronic transaction, it can 'sign' it by means of an electronic signature and then encrypt the whole message, secure in the knowledge that it may be deciphered only by the intended recipient, who will be able to identify the sender.

Cryptography, simply put, is the 'science of codes and cyphers',[6] and involves the application to electronic data of a mathematical algorithm, the encryption' key', in order to render the data indecipherable by anyone not having access to the appropriate decryption 'key'. There are two principal types of cryptography in use, *private* or *symmetric* key cryptography, and *public* or *asymmetric* key cryptography. The way in which these differ is discussed below. In both of

the examples discussed, the sender of the message is Romeo and the recipient Juliet.[7]

Private key cryptography

Figure 1 depicts a *private* or *symmetric* system of cryptography.

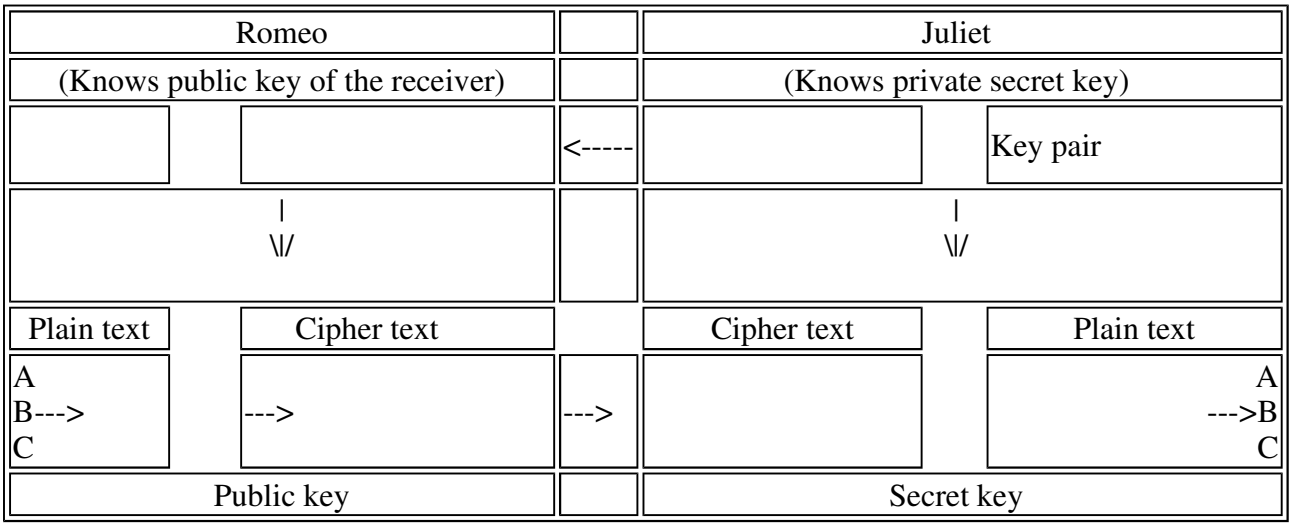


In such a system, both parties have the *same* key, which they keep secret, and this key is used both to encrypt and decrypt any messages sent by the parties. The symmetric system is faster than the asymmetric or public key system, as it uses a smaller number of bits (or digital symbols) in the key (typically 56 to 128).

Various symmetric key algorithms have been in use in recent years, amongst them the Data Encryption Standard (DES), the Fast Encryption Algorithm (FEAL), the International Data Encryption Algorithm (IDEA) and the Secure and Fast Encryption Routine (SAFER). However, some of these may now no longer offer the highest level of security. Philip Zimmermann, the creator of Pretty Good Privacy (PGP),[8] has stated that, with an expensive enough computer system, DES could be cracked in times spanning from 3.5 hours down to two minutes (depending on the size of the computer).[9] Such an enterprise would require a computer costing millions of pounds. However, Zimmermann points out that such a figure could be hidden in the budget of a major corporation tion intentintent on industrial espionage.

Public Key Cryptography

Figure 2 depicts a *public* or *asymmetric* system of cryptography.



In such a system, there is both a *public* and a *private* key, which are a pair. The public key is published, the private key is known only to the individual who generated the key pair. Only the private key fits together with the public key to form a compatible pair.

If Romeo wishes to send Juliet an encrypted message, he encrypts the message using *her public key.* She alone can decrypt it using *her private key* thus the communications contents are secure. This is the process depicted in Figure 2. In addition, though not shown in this figure, Romeo could also have included in the message an electronic signature identifying him as the sender. He would have encrypted this using *his private* key. Once Juliet had decrypted the message contents with her private key, she could have decrypted Romeos electronic signatureusing *his public key*, thus verifying that the message came from Romeo. Had Romeo and Juliet used this system of cryptography, rather than

entrusting their communications to a senile Friar, Shakespeare's story might have had a happier ending.

The disadvantage of public key systems is that they are slower to operate, using larger keys—typically 1,024 bits.

Examples of asymmetric systems which have been in use in recent times are the RSA public key, and the Diffie-Hellmann algorithm. RSA has been embedded in the USA in Microsoft Windows, Netscape Navigator and Lotus Notes amongst other software packages. New products are coming on to the market all the time.

It is possible to speed up asymmetric systems, by using a technique known as a *digital envelope*. This technique combines both symmetric and asymmetric algorithms. An example is the well-known Pretty Good Privacy (PGP) developed by Philip Zimmermann..

Applications of Cryptography

Electronic Signatures

An electronic signature [10] may be described as a string of electronic data used to identify the sender of a data message, in much the same way as a hand written signature a collection of letters scribbled in a particular way identifies an individual. The effectiveness of an electronic signature requires that it be produceable by the sender alone and that any attempt to alter it be incompatible with the integrity of the signature. These qualities of authenticity and integrity can be achieved using cryptography. An electronic signature created using a unique cryptographic private key can only have emanated from the person having control of that key. This of course means that the private key must be guarded securely, much as a physical seal has to be safeguarded against theft.

Encryption

The explanation of cryptography given above sufficiently explains how data may be rendered encrypted and thus confidential. One may encrypt as much or: as little of a message or a document as one wishes. One might wish to encrypt merely the electronic signature at the end of a non-confidential message, so that a specific individual is identified as the sender, or one might wish in addition then to encrypt the whole message, if the intention is to keep the message contents secret.

A problem, however, is that anyone can create an encryption key and claim to be a particular individual. Because of this, unless one knows the person with whom one is dealing, one cannot automatically verify the identity of the sender of a message purely from the electronic signature attached to it. One solution is through the use of an electronic certificate attached to the digital signature. Such certificates are normally issued by bodies known as Certification Authorities (CAs). Such bodies provide certification that an encryption key emanates from the person from whom it purports to emanate. The legislative regulation of such bodies is addressed in the Electronic Communications Act.[11]

THE LAW PRIOR TO THE NEW ACT

Electronic Signatures

Two principal questions arise in respect of the legal status of electronic signatures prior to the coming into effect of the new Act

> (i) where the law does not require a signature to be appended to a document, but an electronic signature has been appended to an electronic document, does this sufficiently identify the purported signer of the electronic document in the eyes of the law?
>
> (ii) where the law requires an individual's signature before a legally binding effect can be achieved, will an electronic signature suffice?

As regards the first question, where there is no legal requirement that there be a signature, there appears to be no objection to a court taking into account an electronic signature as evidence helping to establish that a document emanated from a particular person. Such evidence, if held credible by a judge, could, like any other evidence, help to establish the provenance of a document.

As regards the second question, what if a signature is required by law? Thus far, the law has proved flexible in its estimation of what counts as a signature. In English law, the decision in *Goodman* v. *Eban* [12] established that a

rubberstamp could act as the equivalent of a handwritten signature on a document. Similarly, a faxed signature has been held acceptable.[13] Such decisions have prompted one academic to comment that 'any form of signature will work under English law'. The same consideration would seem to apply to Scots law. [14] It should be added, however, that the cases thus far have at least involved paper documents, and there must remain a question whether the flexibility of the law displayed would extend to non-paper signatures.

A further problem exists, namely that there are few legal provisions which require a signature without also requiring some form of 'writing'. What may constitute 'writing'?[15] The principal rules on writing in Scots law are now contained in the Requirements of Writing (Scotland) Act 1995. The Act states that certain things must be constituted in a 'written document' subscribed by the granter in order to be valid, subscription meaning signing by the granter at the foot of the last page (or for wills, the foot of every page).[16]However, the Act does not say what constitutes a 'written document' or 'writing', so one must look to the Interpretation Act 1978 for assistance. This statute says that writing includes 'typing, printing, lithography, photography and other modes of reproducing words in a visible form, and expressions referring to writing are construed accordingly'.[17]

Thus, even if one could interpret 'signing' to include an electronic signature, it does not seem possible to interpret 'writing' as including electronic documents. The British Government shares this view: 'the Interpretation Act, by placing emphasis on visibility, rules out electronic "writing", which is, in essence, a series of electronic impulses.' [18]For this reason, the Electronic Communications Act addresses both the status of electronic signatures *and* the rules on formal writing.[19]

Encryption

There are no explicit controls currently on the use of encryption to secure the confidentiality of a document's contents. A statutory power is already conferred upon the police in England and Wales to seize computerised data in a legible form, [20]which has prompted debate in England about the necessity of any new powers in this area.[21] Unauthorised efforts to decipher an encrypted document might well occur in circumstances where the document has been unlawfullyintercepted in the course of transmission,[22] or where a computer is being unlawfully used to access the document.[23]

LAW REFORM

Domestic Law Reform

Over the past two years, the British Government has published several documents setting out its intention to reform the law affecting electronic signatures and encryption. In April 1998 the British Government issued a *Secure ElectronicCommerce Statement* setting out its broad legislative views on reform of these areas,[24] of Trusted Third Parties.[25]which followed an earlier 1997 paper addressing the more specific issue The Government began consulting in this area by issuing the consultation document *Building Confidence in Electronic Commerce*[26] The consultation period was remarkably short, one of the many criticisms of the process and proposals made by the House of Commons Trade and Industry Committee in its May 1999 Report, Electronic Commerce: The Government's Proposals[27] The newly formed Performance and Innovation Unit (PIU) of the Cabinet Office also published a report on *Building Confidence in Encryption and Law Enforcement*,[28] which essentially mirrored most of the British Government's proposals in its consultation paper. The Government published its draft Electronic Communications Bill [29]in July 1999. This was followed by consultation on the content, before the publication of a new draft of the Bill in December 1999 after the Committee stage, and then the Bill's introduction into the House of Lords in January 2000. The Bill was finally enacted as the Electronic Communications Act 2000 (hereinafter the "ECA") on 25 May 2000. The Government's view is that the provisions in this new legislation for the recognition of electronic signatures will have to conform with the parameters of the European Directive on a Community framework for electronic signatures,[30] and: the final text of the draft Directive on electronic commerce.[31]

Electronic Signatures

Validity/Admissibility

The British Government originally proposed creating rebuttable presumptions that would apply to certain electronic signatures[32] .However, they were persuaded that this was a bad idea.[33] The current terse proposal on electronic signatures is now contained in section 7 of the ECA:

> **7.- (1) In any legal proceedings (a) an electronic signature incorporated or logically associated with a particular electronic communication or with particular electronic data, and**

> **(c) the certification by any person of such a signature, shall each be admissible in evidence in relation to any question as to the authenticity [34]of the communication or data or as to the integrity [35]of the communication or data.**

The British Government has thus chosen to address the validity of electronic signatures in terms of their evidential admissibility, rather than via a blanket statement that electronic signatures are legally valid. This contrasts with the approach taken in other legislation, such as the US Electronic Signatures in Global and National Commerce Act (the E-SIGN Act)36(a)[36] the Uniform Computer Information Transactions Act (UCITA)[37] and the Uniform Electronic Transactions Act (UETA),the Australian Electronic Transactions Act 1999, [38]and the EC Directive on a common framework for electronic signatures,[39] which do contain a general statement as to the validity of electronic signatures.

The provisions of section 7 apply to all electronic signatures, not simply those issued by approved providers and regardless of the jurisdiction in which the signature was issued. However, because the provision merely says electronic signatures are to be admissible in evidence, and does not provide that they create any presumptions as to the provenance, authenticity or date of any data carrying an electronic signature, it will be for parties to lead evidence on these issues.[40] Similarly, the US provisions do not provide for any presumptions, though they provide a little more guidance on the circumstances to be considered. UETA allows the identity of the author of an electronic record or signature to be 'shown in any manner',[41] and provides for the effect of such data or signature to be determined 'from the context and surrounding circumstances',[42] while UCITA provides that the court is to consider the commercial reasonableness of the technology used.[43]

Requirements of Writing

As regards the equivalence of an electronic signature to a handwritten signature for the purposes of requirements of writing, the British Government has chosen to leave this to secondary legislation. The provisions of the ECA allow, the relevant Government Minister,[44] to amend legislation by statutory instrument 'in such manner as he may think fit for the purpose of authorising or facilitating the use of electronic communications or electronic storage (instead of other forms of communication or storage)' [45]for any of various specified purposes.[46] This will leave it to Ministers to decide, for instance, whether one will be able to make an electronic will or to transfer heritable property by electronic disposition. Whether the signatory of, for instance, a will would also require to find an electronic witness in order to render the will probative [47] is an unknown factor. It may be that the Government's view would be to the effect that the certificate of a Certification Authority would suffice. In respect of wills, however, regard will no doubt be had to the provisions of the Directive on electronic commerce, when it is eventually finalised. In Article 9 of the most recent draft, [48] Member States are given power to exclude certain categories of transaction from the general principle upholding electronic contracts. The categories include contracts creating or transferring rights in real estate (excluding leases), and contracts governed by family law or succession (which would include wills).

We must thus wait to see to what extent British or Scottish Government Ministers decide to amend existing statutory requirements relating to the requirements of writing. The US drafters of UETA have taken a bolder step. Their provision simply states: '[i]f the law requires a record to be in writing, an electronic record satisfies the law'.[49]

There is one further crucial aspect to note concerning the power of amendment delegated to Ministers. That is, that any such amendment may include provisions concerning the determination of whether a thing has been 'done' using electronic communication or storage, and, where something has been so done, the time and place at which it was done, the person by whom it was done, and the contents, authenticity and integrity of electronic data. This means that while the provision of the ECA generally recognising the admissibility of electronic signatures [50]contain no guidance on how a court is to adjudicate on such issues as time and place of signature, authenticity of contents, and so forth, individual pieces of delegated legislation may contain particular rules for particular areas of law. The wisdom of such a scheme, entailing as it does the potential for conflict, is doubtful, and may result in confusing legal differences.

Cryptography

The ECA creates a *voluntary approvals regime* to cover providers of all cryptography support services',[51] not just for those providing certificates in respect of electronic signatures. Other services might include the storage of encrypted data, and the provision of key escrow and key recovery. These latter two are variations on a theme, allowing a key which has been lost either to be replaced with a copy held by an agency (key escrow) or to be rebuilt by the agency (key recovery). Such agencies are often referred to as Trusted Third Parties (TTPs).[52]

The purpose of the Register is to build confidence in electronic commerce, by providing a list of agencies which have met approval conditions upon which consumers will be able to rely in purchasing cryptography support services. The ECA permits assessment of compliance with the approval conditions to be carried out by a person specified by the Secretary of State,[53] thus allowing him to appoint an expert in cryptography to assist with this function.

In its earlier consultation document, the British Government set out the conditions which it expected agencies to have to meet before they would be certified [54]by the person or body supervising these arrangements.[55] These were strongly criticised by the Trade and Industry Committee as 'not fit to be written into law'.[56] The British Government has, however, rejected this criticism, though the exact criteria which agencies will have to meet have not been specified in the ECA. It has been left to the Secretary of State to ensure that arrangements are in force for granting approvals to those seeking inclusion in the Register of approved providers,[57] and we must await the publication of these requirements in due course.

The British Government's earlier intention to require certified agencies to offer key escrow as part of their services, or at least to promote key escrow,[58] has now been abandoned.[59] This followed heavy criticism of key escrow from many parties, including the Trade and Industry Committee, who commented that '[w]e are disappointed . . . that the Government should still hold a candle for key escrow and key recovery'.[60] The final blow was a distinct lack of enthusiasm for key escrow from the Cabinet Office PIU. However, in the text of the ECA as passed a provision which will enable Ministers to include within subordinate legislation a requirement that a key be deposited with an intended recipient of electronic communications, or, as an alternative, for arrangements to be made to ensure that encrypted data do not become unusable through key loss. It is unlikely that the imposition of such a requirement could assist electronic commerce. The Government may have had in mind here the possibility of utilising this provision in relation to the submission of official forms and documentation, though the requirement to deposit a key seems to be a recipe for slower communication, something which electronic communication with government departments was supposed to improve!

Liability of Providers of Cryptographic Services

A major issue on which the British Government consulted was the liability of Certification Authorities (CAs) and other providers of cryptographic services for losses caused by them. Such losses may occur, for instance, through the issuing of a certificate to the wrong party. The Trade and Industry Committee recommended that in the current 'nascent market' the Government 'exercise caution' [61] in instituting a statutory liability regime. In drafting the ECA, how-ever, the British Government will have had to bear in mind that Article 6(1) of the EU Directive on electronic signatures requires that 'Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public, a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate'.

Given this European background, it might be thought surprising that the British Government has decided that 'the liability of Trust Service Providers (TSPs) both to their customers and to parties relying on their certificates, is best left to existing law and to providers' and customers' contractual arrangements'. [62]Customers will certainly be able to look to their contracts, though these will be subject to exclusion and limitation clauses,[63] but what of the position: of third parties? Such parties will have to rely on the law of delict/tort, arguing misrepresentation along *Hedley Byrne* lines,[64] or perhaps (in Scotland) arguing for a *jus quaesitum tertio* (third party right) in their favour, though this is more unlikely. The impression is given that the British Government considers the existing law adequate to meet its European obligations, though whether it has thoroughly considered this issue may be doubted.

There is also the question of the liability of the holder of a private key, should the key's secrecy become compromised, another use it, and loss be caused. This would not constitute misrepresentation, but could arguably be negligent, though if the result were pure economic loss then recovery would be unlikely.[65] The Bill does not address this issue of the liability of private key holders.

Law Enforcement Agency Access

The most thorny issue on encryption is probably that of law enforcement access to encrypted material and keys. A startling change between the first and second drafts of the Electronic Communications Bill was the removal of the law enforcement provisions contained in the first draft, and their subsequent re-insertion into the Regulation of Investigatory Powers Act 2000 ('the RIP Act').[66] The decision to remove these provisions from the ECA was undoubtedly influenced by criticism from various bodies, including the Trade and Industry Committee, which had commented that it was 'unfortunate that legislation to deal with the recognition of electronic signatures in law, and related measures, should have become entangled with the requirements of law enforcement agencies to tackle criminals' use of encryption'.[67]

The provisions of the RIP Act include a power for law enforcement agencies [68] to require disclosure of a decryption key [69]necessary to access protected information. [70]This power is exercised by serving a notice of disclosure on the person holding the key. Such a notice can be served only after obtaining permission to do so from the appropriate judicial authority[71]. Key disclosure may be required by law enforcement agencies if they reasonably believe that such access is necessary on grounds of national security, the purposes of preventing or detecting crime, or in the interests of the economic well-being of the country. Disclosure may also be compelled if it is necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty',[72] an extremely wide justificatory reason, which seem to cover a whole range of public authority duties and powers, many with

little or no connection to the more specific over-riding interests stated. Section 50 spells out the effect of a disclosure notice being issued. If the person to whom it is addressed has both the encrypted information and the key, that person may use the key to make the information intelligible and is required to disclose *either* the information in an intelligible form [73] or the key. [74] If the addressee has the key, but not the encrypted information, he must disclose the key. [75] It is possible for the law enforcement agencies to ask that only disclosure:of the key will meet the requirements of a disclosure notice. The relevant judicial authority [76] may only grant such a request if there are special circumstances which would otherwise mean that the purposes for which the request was made would be defeated, and if the direction would be proportionate to the goal sought to be achieved.[77] This caveat will allow a police officer to convince a judge that investigation of a crime would be compromised unless the key itself were obtained. Cautious police officers might well be likely to ask for this direction every time. It remains to be seen whether the judiciary will challenge such a request if it becomes standard practice.

The provisions on access to encryption keys may be seen to be wide, and whilst there is some provision for supervision of the persons who obtain keys under the provisions,[78] the law enforcement access provisions of the Act have come in for stiff criticism from advocates of personal privacy and freedom of e-commerce.[79] The most strident criticism has been reserved for the new criminal offences which the Bill will create, namely an offence of not complying with a disclosure notice (section 53) and an offence of tipping off another person about a disclosure notice (section 54).[80]

THE INTERNATIONAL DIMENSION

Export Controls

The Wassenaar Arrangement

Certain cryptographic products are treated as restricted dual-use technology under the Wassenaar Arrangement.[81] Under this international agreement, signed by 33 nations (including the United Kingdom and the United States of America), the export of certain cryptography is subject to restrictions similar to those applicable to munitions.

The Wassenaar controls apply to the transfer of conventional arms and dual-use goods and technologies, dual-use technologies being those capable of use both for innocent and non-innocent purposes. Participating states are required to control all items set out in the list of dual-use technologies and munitions.[82] Cryptography falls under the dual use list, [83] though not all cryptography is con-trolled. The list specifies the types of symmetric and asymmetric algorithm that are caught, which includes RSA and Diffie-Hellmann.

Section I.4 of the Arrangement states that the provisions on cryptography will not impede *bona fide* civil transactions, though this is an assertion challenged by civil libertarian groups.[84] It should be noted, however, that the Arrangement does not say that *possessing* cryptography must attract sanctions, but only the transfer of it across national boundaries.

United Kingdom Controls

In the United Kingdom, the current export controls imposed under the Export of Goods Control Order 1994 [85] and the Dual-Use Items (Export Control) Regulations 2000 [86] mirror the provisions in the Wassenaar Arrangement as regards the types of cryptography caught. The new 2000 Regulations replace previous 1996 regulations, and were introduced to comply with the terms of the EC Regulation for the control of export of dual-use items and technology [87] which took effect on 18 September 2000. Unlike the prior UK regulations, the new regulations cover the export of items in both tangible and intangible form. Thus, whereas previously exports of cryptographic technology on paper (for instance, setting out on paper a cryptographic algorithm) or on computer disc were caught by the regulations, but export via file transfer on the internet was not, the latter will now also be subject to export control.

The USA

The abandoned attempt by US law enforcement agencies to prosecute Philip Zimmermann for breaking export controls with respect to his PGP, testifies to the level of governmental concern about the potential use of cryptography by criminals. However, given that the Wassenaar restrictions apply only to exports across national borders (and it is therefore not illegal to distribute *within* the signatory states those products which it would be illegal to export), and given the ease of evading export controls and transferring software internationally via the Internet, the drafters of Wassenaar appear somewhat like King Canute holding back the waves.[88]

The US Department of Commerce issued new encryption export regulations in January 2000. The status of these regulations may, however, be affected by a US Court of Appeals decision 89(a) that computer source code is a form of speech and thus protected by the First Amendment.

International and Supra-national Proposals for Law Reform

As the British Government note in *Building Confidence* [e]lectronic commerce is essentially a global, rather than a national, issue'.[89] The ECA purports to have been drafted with supranational proposals in mind. Such supranational proposals include the EU Directive on electronic signatures,[90] the proposals fromthe Organisation for Economic Co-operation and Development [91] and the United Nations Commission on International Trade Law,[92] and the US Computer Information Transactions Act (UCITA)[93] and Uniform Electronic Transactions Act (UETA).[94] The ECA is generally in conformity with the requirements of the Directive on electronic signatures. Indeed, in some ways it goes further. For instance, under the Directive, Member States are not required to set up a voluntary licensing scheme, though the Act does so.

On the international stage, other governments have been producing legislative proposals in this field also. Amongst them, the Australian [95]Parliament has recently promulgated an Electronic Transactions Act; the Singaporean Government has promulgated the Electronic Transactions Act 1998;[96] and the Irish Government is about to publish a Bill dealing with electronic signatures and related e-commerce matters.[97]

CONCLUSIONS

The area of cryptography, like all areas of information technology, is fast moving, and law reform is always at least three steps behind. Commentators in this field find themselves much like on-the-spot television reporters, narrating events as they unfold without much opportunity to sit back and assess the longer-term perspective. Bearing this in mind, what comments are possible on the proposals for law reform in this country?

There is a danger that both the EU Directive and the UK provisions for the recognition of electronic signatures, by tying themselves to a technology based upon public key cryptography, will run the risk of requiring a radical overhaul in a short timescale. There is much to be said for a more technologically neutral approach, such as that adopted in UCITA. [99]That said, the British Government has committed itself to an approach based on electronic signatures. The old law of signatures and writing was clearly outmoded, and the reforms will provide a somewhat belated legal recognition of the existing use of electronic media in business and consumer transactions.

Then there is the issue of law enforcement access to encryption, now addressed in the Regulation of Investigatory Powers Act. Whilst some steps must no doubt be taken, to show a determination to act, if for no other reason, the ready availability of strong encryption techniques and the ease with which encrypted documents may be transferred will no doubt mean that most intelligent criminals are able to avoid the long arm of the law. In practice, new provisions are unlikely to make more than a minimal impact in crime prevention and detection, and may simply be perceived as rendering the United Kingdom less attractive as a forum for the conduct of e-commerce.

The widespread use of computers and the Internet has made encryption avail-able worldwide for the majority of computer users, as more and more software packages come with built-in encryption technology. This ever increasing avail-ability is certain to provoke continued heated exchanges between those concerned at the prevention of crime and those favouring privacy protection. What is almost as interesting in this area as the legal developments, however, is the extra-legal pressure exerted in the attempt to achieve overt or covert access to encrypted material by law enforcement agencies.[98]

In the field of cryptography, the fluctuating consensus between government, business and private individuals will be formed less often within the parameters of the legal world and more often within those of the online community; it will be driven less by politicians and law reformers, and more by individual computer users. The British Government is aware of the importance of self-regulation in the area of the provision of cryptography support services. This is not surprising, for the spotlight of the law only shines so far into the information technology ether.

* Lecturer, The School of Law, University of Edinburgh.

---

[1] Or 'digital signatures' as they are also referred to

[2] Notably, in the responses to the DTI's Consultation Paper, *Building Confidence in Electronic Commerce, A Consultation Document* (Mar. 1999), and the witness interviews conducted as part of the House of Commons Trade and Industry Committee's investigation of Electronic Commerce (whose Report was published on 12 May 1999).

[3] The Electronic Communications Act 2000. c.7, available at http://www.hmso.gov.uk/acts/: acts2000/20000007.htm. For the consultation paper issued prior to the Act, see *Promoting Electronic*Commerce: Consultation on Draft Legislation (Cm 4417, The Stationery Office, London, July 1999), available at <http://www.dti.gov.uk/cii/elec/ecbill.pdf>. The Bill was amended by the House of Commons in Committee on 16 Dec. 1999, and subsequently introduced into the House of Lords on 26 Jan. 2000. The current text of the Bill is available at: <http://www. parliament. the-stationery-office. co.uk/pa/ld199900/ldbills/024/2000024.htm>

[3a] <http://www.hmso.gov.uk/acts/acts2000/20000023.htm>.

[4] Although with handwritten signatures forgery is not unknown.:

[5] Although changes to documents after signature are normally accompanied by a further signature: next to the alteration, it is not impossible to alter a paper document without detection.

[6] *Ibid.,* 17.

[7] The diagrams are taken from the European Commissions' paper, Towards a European Framework for Digital Signatures and Encryption (8 Oct. 1997), which may be found at <http://www.ispo.cec.be/eif/policy/ 97503toc.html

[8] See the mention of this in the section on public key cryptography below.

[9] See Philip Zimmermann's testimony before the United States senate: <http://www.nai.com/products/security/phil/phil-quotes.asp>

[10] Defined in the text of the Electronic Communications Act, s. 7(2) as: 'so much of anything in electronic form as—
(a) is incorporated into or otherwise logically associated with any electronic communication or electronic data; and
(c) purports to be so incorporated or associated for the purpose of being used in establishing the authenticity of the communication or data, the integrity of the communication or data, or both.'
In the first draft of the Bill, the definition of electronic signature included the requirement that the signature be 'generated by the signatory or other source of the data'. The final text as passed omits: the requirement, and it thus seems that a signature could emanate from a third party and still fall within the definition.

[11] See below for the relevant provisions.

[12] [1954] QB 550

[13] *In Rea Debtor* (No 2021 of 1995) [1996] 2 All ER 345.

[14] See the Trade and Industry Committee's Report (May 1999), para. 41, quoting the opinion of Chris Reed of Queen Mary and Westfield College, available at <http://www.parliament.the-stationery- office.co.uk/pa/cm199899/cmselect/cmtrdind/187/18702. htm>

[15] This issue is dealt with further in the specific context of electronic contracts in Murray, *supra* p. 19

[16] See for more details, the Requirements of Writing (Scotland) Act 1995, c.7, s 1.

[17] Interpretation Act 1978, c.30, s 5, Sch. 1.

[18] *Building Confidence,* para. 16.

[19] See below.

[20] In England and Wales under the Police and Criminal Evidence Act 1984 (PACE), ss. 19(4) and

[21] The Law Society of England and Wales appears to be of the opinion that no new powers are needed (see Trade and Industry Committee Report, para. 99 (n. 28 below)) due to existing powers in England and Wales under PACE.

[22] See the Interception of Communications Act 1985.

[23] See the Computer Misuse Act 1990, ss. 1–3.

[24] See <http://www.dti.gov.uk/CII/ana27p.html>.

[25] See <http://dtiinfo1.dti.gov.uk/cii/encrypt/>.

[26] See <http://www.dti.gov.uk/cii/elec/elec_com.html>.

[27] See <http://www.parliament.the-stationery-office.co.uk/pa/cm199899/cmselect/cmtrdind/187/18702.htm>.

[28] See <http://www.cabinet-office.gov.uk/innovation/1999/encryption/index.htm>.

[29] See n. 3 above.

[30] Dir. 1999/93/EC, see <http://europa.eu.int/comm/dg15/en/media/sign/Dir99-93-ec%20EN.pdf>.

[31] For the latest text, see document 14263/1/99 REV 1, issued on 28 Feb. 2000.:

[32] Namely, that the electronic signature identified the signatory it purported to identify, and secondly, where the signature purported to guarantee that the accompanying data had not been altered since signature, that they had not been so altered.

[33] This argument was forcefully put by, amongst others, the T&I Committee. The two main points it made were (1) that to create two tiers of signature—those that would qualify for the presumptions and those that would not—was alien to an English law approach, and (2) that it would reverse the burden of proof, thus undermining confidence in electronic commerce.

[34] S.15(2)(a) defines references to the authenticity of any communication or data as references to whether the communication or data come from a particular person or other source, is accurately timed and dated, and/or is intended to have legal effect.

[35] S. 15(2)(b) defines references to the integrity of any communication or data as 'references to whether there has been any tampering with or other modification of the communication or data'.

36(a) This Act was signed by the US President on 30 June 2000 and takes effect on 1 Oct. 2000. An electronic version is available at the http://thomas.loc.gov website.

[36] The UCITA provision (s. 107(a)) states: 'A record or authentication may not be denied legal effect or enforceability solely because it is in electronic form'. For details on UCITA see <http://www. 2bguide.com>. The text of the Act is at <http://www.law.upenn.edu/bll/ulc/ucita/cita10st.htm>.

[37] The UETA provision (s. 7(d)) states simply: 'If a law requires a signature, an electronic signature satisfies the law'. For details on UETA see <http://www.webcom.com/legaled/ETAForum/>. The text of the Act is at <http://www. law.upenn.edu/bll/ulc/fnact99/1990s/ueta.htm>.

[38] See http://scale.puls.law.gov.uk/html/cornack/10/6074/rtf/162of99.rtf. Section 8(1) reads: 'For the purposes of a law of the Commonwealth, a transaction is not invalid merely because it took place wholly or partly by means of one or more electronic communications'. Cl. 9 provides for the use of electronic communications to meet writing requirements, and section 10 states the requirements which electronic signatures must meet to be valid.

[39] Art. 5(2) of which states that 'Member states shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:—in electronic form . . .'. One may also note the latest draft (from the Parliament and the Council) of the Dir. on electronic commerce, Art. 9 of which reads: 'Member States shall . . . ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means'. See http://europa.eu.int/eur-lex/ en/tif/dat/1999.en_399L0093.html.

[40] The Westminster Government was stated that '[i]t will be for the court to decide in a particular case whether an electronic signature has been correctly used and what weight it should be given': see Commentary on Cl.s in *Promoting Electronic Commerce* (Cm 4417, The Stationery Office, London), 22

[41]. UETA, s. 9(a).

[42]UETA, s. 9(b).

[43] UCITA, ss. 108, 114 and 212

[44] As to which see s. 9(7).

[45] S. 8(1).

[46]They are specified in s. 8(2), and include the doing of anything which is required to be done in writing or otherwise using a document, notice or instrument, and the doing of anything which is required to be or may be authorised by a person's signature or seal, or is required to be witnessed.

[47] That is to say, to gain the benefits of certain presumptions specified in s. 3 of The Requirements of Writing (Scotland) Act 1995.

[48] 28 Feb. 2000: Common position of the Council and Parliament (14623/1/99 REV 1)

[49]. UETA, s. 7(c).

[50] That is, s. 7.

[51] S. 2(1)(a). The term is defined in s. 6(1) as meaning: 'any service which is provided to the senders or recipients of electronic communications, or to those storing electronic data, and is designed to facilitate the use of cryptographic techniques: for the purpose of—
(a) securing that such communications or data can be accessed, or can be put into an intel-ligible form, only by certain persons; or
(c) securing that the authenticity or integrity of such communications or data is capable of being ascertained.'

[52] The Government referred in *Building Confidence* to Trusted Service Providers (TSP) as an umbrella term to describe an agency choosing to offer any cryptographic service, whether it be as a CA or TTP.

[53] S. 2(4).

[54] See *Building Confidence,* Annex A.

[55] The conditions for the appointment of such supervising person or body are set out in s. 3. The Government has proposed that these functions will be delegated to OFTEL.

[56] T&I Committee Report, para. 73.

[57] See s. 2(1).

[58] Though the Performance and Innovation Unit concluded in their report (May 1999) that 'wide-spread adoption of key escrow was unlikely in the current industry and climate' (para. 6.9).

[59] There is a specific prohibition against a requirement for key escrow as a prerequisite for inclusion on the register of approved cryptography service providers: s. 14(1)(a).

[60] T&I Committee Report, para. 90.

[61] T&I Committee Report, para. 79.

[62] *Promoting Electronic Commerce* (Cm 4417, The Stationery Office, London), 2.

[63] Which in turn, however, are subject to the provisions of the Unfair Contract Terms Act 1977 and the Unfair Terms in Consumer Contracts Regs. 1999, S.I. 1999 No. 2083.

[64] That is to say, basing their argument on the principle laid down in *Hedley Byrne & Co Ltd v.Heller & Partners Ltd* [1964] AC 465. There appears to be a strong case to support liability based on this principle, as the whole purpose of a certificate is for third party reliance.

[65] There is also a question whether a certificate or a key constitutes goods. This question has relevance with respect to liability under the Sale of Goods Act 1979 and product liability under the Consumer Protection Act 1987. The answer is unclear. It is not certain whether computer software constitutes goods (see MacQueen, Hogg and Hood, *Muddling Through: Legal Responses to E-Commerce* from the Perspective of a Mixed System (Europees Privaatrecht 1998, Molengraaff Instituut). A key is an algorithm and a certificate a statement of the identity of a key-holder. Neither seems to bear much resemblance to a 'good'.

[66] <http://www.hmso.gov.uk/acts/acts2000/20000023.htm>. The Scottish Parliament has also passed a Regulation of Investigatory Powers (Scotland) Bill. However, this Scottish bill does not include provisions on decryption, as this issue is dealt with for the whole of the United Kingdom in the RIP Act. For the text of the Scottish Bill see http://www.scottish.parliament.uk/ parl_bus/billsb16bsl.pdf.

[67] T&I Report, para. 116.

[68] Amongst others. On the categories of persons who may require access, see s. 46(1) of the RIP Act.

[69] The Act excludes keys which are intended to, and do, only create electronic signatures, rather: than encrypted text: see *ibid.,* s. 49(9).

[70] *Ibid., s.* 49. Protected information is defined in s. 56 as, broadly, encrypted electronic data.

[71] On the appropriate judicial authority, see Sched. 2, *ibid*.

[72] *Ibid.,* cl. 46(2)(b)(ii).

[73] The Government suggested that an example of a situation where this might apply would be to "allow a company—that might have received an encrypted message from the target of a particular enquiry (e.g. a criminal)—to offer up an intelligible copy of the message (e.g. a printed copy) rather than the decryption key" *(Promoting Electronic Commerce*, 24). Could such a decrypted message be proven to be accurate? There are various ways of demonstrating this. For instance, the document as de-encrypted could be re-encrypted with the public key, and this re-encryption could be compared with the original encrypted document. If the two are the same, then the de-encryption was accurate.

[74] S. 50(1),(2)

[75] S. 50(3)(a).

[76] As to which, see Schedule 2 to the Act.

[77] S. 51(4)

[78] *Ibid.,* s. 55.

[79] The provisions have been criticised by, amongst others, STAND and the Foundation for Information Policy Research. See, also, the interesting scenarios suggested by Lindsey, which he uses to criticise the provisions on law enforcement access, available at <http://www.cs.man.ac.uk/~chl/ scenarios.html>.

[80] Not all disclosure notices are affected by an obligation of secrecy: for those that are, see s. 54(2)(3) of the Act.

[81] See <http://www.wassenaar.org/>.

[82] s.III.1.

[83] In category 5, part 2, Information security.

[84] See, for instance, the arguments advanced at <http://www.gilc.org/crypto/wassenaar/>.

[85] SI 1994 No. 1191, as amended.

[86] SI 2000 No. 2620.

[87] EC Council Regulation 1334/200, available at <http://europa.eu.int/eur-lex/en/lif/dat/2000/en_300R1334.html>.

[88] The Trade and Industry Committee also expressed its scepticism about the value of export controls, and recommended that 'the Government consider the case for a review of the rationale for the continuation of export controls on cryptographic products, in the light of their widespread availability' (T&I Report, para. 112).

89(a) *Junger v. Daley,* US Court of Appeals, 6th Circ., 4 April 2000, see http://pacer.ca6.uscourts.gov./cgi-bingetopn.pl?OPINION=00a0017p.06

[89] Para. 6.

[90] See <http://europa.eu.int/eur-lex/en/lif/dat/1999/en_399L0093.html>.

[91] See their Guidelines on Cryptography Policy at <http://www.oecd.org/dsti/sti/it/secur/prod/e-crypto.htm>.

[92] See their Model Law on Electronic Commerce at <http://www.uncitral.org/english/texts/elect-com/ml-ec.htm>.

[93] Previously proposed as new Art. 2B of the Uniform Commercial Code. See <http://www.2bguide.com/>.

[94] For details on UETA see <http://www.vetaonline.com>. The text of the Act is at <http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta.htm>.

[95] The Electronic Transactions Act 1999. See <http://scalepuls.law.gov.au/html.comact/10/6074/rtf/162of99.rtf>.

[96] The Electronic Transactions Act 1998. See <http://www.cca.gov.sg/eta/index.html>.

[97] See <http://www.entemp.ie>.

[99] That is, leaving it to the parties to decide which technology to use, subject to a court's deter-mination of the commercial reasonableness of such technology: see the discussion of this in the main text at p. 45 above.

[98] A classic example of covert, or at least quasi-covert, law enforcement access is a recent well-publicised liaison between certain security agencies of the US Government and software producers. An example of this relates to the National Security Agency in the USA, which managed to ensure that the cryptography bundled with some software systems exported from the USA provided less security than users might have thought. Netscape and Microsoft, for instance, have both altered their net browsers' security systems, SSL, which are used to encrypt Internet credit card transactions amongst other things, so that 88 of the 128 bits of the encryption are broadcast at the start of the transaction. The remaining level of security, 40 bits, means that so-called 'secure' web transactions may be read by signals intelligence computers. The Swedish Government was caught out with a similar: problem affecting the Lotus Notes e-mail system they purchased for all government employees. It believed that the 64-bit key provided relative security. In fact, the version it was using extracted 24 bits of each key and passed it to the NSA in America. When questioned, Lotus openly admitted that it had modified the program in this way.