Draft Bill on ELECTRONIC COMMUNICATIONS

Published on 23 July 1999

Response by the Law Society

INTRODUCTION

The Law Society recognises that the draft Bill is a welcome attempt to clarify ambiguities in the electronic commerce consultation paper, *"Building Confidence in Electronic Commerce"*[1]. It still feels however, that three areas of the Bill are problematic and must be addressed quickly.

- The draft Bill seeks both to regulate the e-commerce market and to provide for law enforcement access. In the same breadth it tries to encourage the development of e-commerce while laying down heavy-handed arrangements for law enforcement access. This approach will send mixed signals about the openness of the UK e-commerce market and may cause e-commerce users to go elsewhere.

  Lawful interception of electronic communications, by law enforcement agencies, should be addressed in separate legislation, following an entirely separate consultation process.

- The role given to the executive, throughout the Bill, is too prominent. Consumers and industry will rightly have concerns about conflict of interest and implications this may have on the right to privacy and to a fair trial.

- There are still provisions which are inconsistent with the Government's stated aim of producing a technology neutral Bill. The Government's clear rejection of Key Escrow offers some reassurance to industry and consumers about the Government's intentions. However, as outlined in the attached response, provisions regarding Certification Agencies and possible conditions on electronic access to Government services are not satisfactory.

- To emphasise the Government's commitment to developing electronic commerce, the title of the Bill should specifically mention "electronic commerce".

[1] Published on 5 March 1999.

PART 1 CRYPTOGRAPHY SERVICE PROVIDERS

A number of jurisdictions have adopted a flexible legal framework for e-commerce in an effort to allow this new market to grow. Australia and Bermuda, for example, have decided not to provide for the licensing of cryptography services providers and to base their e-commerce legislation on the UNCITRAL Model.

The Law Society suggests that the UK also abandon the aim of regulating certification agencies. As yet, no convincing case has been made for the need to regulate the provision of certification or other encryption services, and the importance of such services for the development of electronic commerce remains a matter of speculation. Accordingly, the Law Society would favour the removal of the entirety of Part I of the proposed Bill.

If Part I of the Bill remains, the Law Society makes the following suggestions.

Clause 1 and 2 : Register and grant of approvals for service providers

The Society recognises that the draft Bill has taken a positive step in abandoning the misleading terms "licensed" or "unlicensed" Certification Agencies as they imply a permission to carry out an activity that would otherwise not be permissible. Nevertheless, the Bill's use of the terms "approved" or "unapproved" may mislead the consumer into thinking that unapproved agencies are really "disapproved" and should not be used. The Society considers that it is important to avoid loaded terms of this kind, and suggests that "registered" and "unregistered" are suitably neutral.

Although the Government has indicated that a statutory scheme is an option to be held in reserve, Clause 1(1) imposes a duty on the Secretary of State to establish a register. Although this part might never be brought into force, the Society urges that Clauses 1(1) and 2(1) emphasise that the registration scheme is voluntary.

The Society regards the powers granted by Clause 2 as excessively wide. Given the uncertainty about what regulation is really needed, and the considerable past concern about the Government's objectives in proposing mandatory schemes, such wide powers will lead to uncertainty about how they will be exercised. This is undesirable if the UK is to become a prime location for electronic commerce.

The Society urges that the powers provided for at Clause 2 should not be exercisable except after investigation and report by the Competition Commission (or some other suitably independent body) based on published evidence and following public hearings. The powers should be exercisable only for the purposes of remedying shortcomings identified in the report.

PART II FACILITATION OF ELECTRONIC COMMERCE, DATA STORAGE ETC.

Clause 7: Electronic signatures and related certificates

1. Legal value of electronic signatures and writing

Clause 7 (1): provides that:

> " In any legal proceedings-
> (a) an electronic signature incorporated or logically associated with a particular electronic communication, and
> (b) the certification by any person of such a signature,
>
> shall each be admissible in evidence in relation to any question as to the authenticity of the communication or its integrity."

- Electronic signatures are already widely regarded by lawyers as admissible. If the purpose of this clause is to reassure the fainthearted it fails to achieve its aim. The clause refers only to " communications" and creates unnecessary doubts regarding its scope. Although the intention is surely for the term to include contracts and agreements, the Bill altogether fails to deal with Deeds, which have a special status under English law as self-proving documents. Is it the intention that Deeds may be created electronically?

- The admissibility of electronic signatures should not be limited to questions relating to authenticity or integrity of communications. Equivalence between electronic and traditional communications requires electronic signatures to be admissible for "any question as to the authenticity of the communication or its integrity or otherwise". An electronic signature may, therefore, be admitted as evidence not just in relation to the source and integrity of what is signed, but as evidence that it is in fact signed, with all the same significance that the common law attaches to the fact of signature.

- The Law Society believes that clause 7(3) does not correctly reflect available procedures for certification. What is certified is neither a signature nor a procedure, it is a verification key used in a procedure to verify a signature.

2. The burden of proof in electronic communications

Despite abandoning the onerous "rebuttable" presumption put forward by the consultation paper, **Clause 8(4)(d)** of the draft Bill would enable such a presumption to be reintroduced. The Law Society repeats its view that the Government should adopt the approach in the draft Australian legislation on electronic commerce.

The latter states that, unless otherwise agreed between the purported sender and the recipient of an electronic communication, the purported sender of the electronic communication is bound by that communication only if it was sent by the purported sender or with the authority of the purported sender. Secondary legislation should not enable this approach to be reversed.

3. Contract law

1. Consumer Credit Act

The Society suggests that the Government extend the scope of Section 75 of the Consumer Credit Act 1974 so that the cardholder protection extends to transactions overseas covers use of debit cards as well as credit cards. Electronic commerce will obviously involve frequent transaction overseas and such a measure would certainly contribute to promoting consumer confidence in electronic transactions.

2. Taxation issues

The Society welcomes the Government's statement[2] that it will not introduce new taxes on electronic commerce[3] but is concerned that uncertainty about electronic transactions mean that the Tax Authorities could introduce changes to existing rules.

Tax Authorities believe, for instance, that they need more rules to tackle taxpayers who may use the Internet to conceal their identity or who use electronic record-keeping systems in order to leave an audit trail which easy to alter. They also feel that current rules do not allow them to apply "paper" concepts, such as permanent establishment, to electronic commerce users.

Any burdensome fiscal environment for e-commerce users will result in them relocating abroad. To avoid this danger, no fiscal changes specifically related to electronic transactions should be made without close prior consultation with industry and consumer groups.

3. Export control

The Law Society notes with concern that the Government has said the revised Wassenaar arrangements (which set international export controls on encryption) will soon be implemented in the UK.

Maintaining current export control procedures on encryption will have serious adverse effects on the development of the e-commerce market in the UK. If controls were extended to intangible exports, they might even frustrate international collaborative efforts to improve cryptographic computer system security. The Wassenaar arrangements should not be used to impede the development and deployment of cryptography for civil computer system security.

Clause 8: Power to modify legislation

Clause 8 gives Ministers extensive powers to modify e-commerce legislation by statutory instrument

> "(..) for the purpose of authorising or facilitating the use of electronic communications or electronic storage (..)".

The Society believes that the scope of ministerial powers described at Clause 8 (1) to (7) is far too wide. If applied, the clause would enable Ministers to regulate the e-commerce market without having to engage in any consultation process with industry or with consumers. Ministers could disregard the results

[2] Statement Issued by the Inland Revenue and Customs & Excise in October 1998.

[3] The Law Society is aware that, in May 1998, the World Trade Organisation (WTO) adopted a Declaration on Global Electronic Commerce which provides that member countries "will continue their current practice of not imposing customs duties on electronic transmissions". It is also aware that this situation will continue until the next WTO Ministerial Conference in 1999.

of consultations during the drafting of the Bill and reintroduce controversial measures such as Key Escrow or Third Party Key Recovery by the back door. Whatever assurances are given that Ministers are unlikely to take such measures (because these would amount to "killing-off" the UK e-commerce market) consumers will say that a market where the legal framework is open to uncontrolled change is unattractive.

Clause 8 would not be necessary at all if the legal value of electronic writing and signatures were adequately clarified.

In its response to the DTI's consultation document, the Law Society suggested that the definition of the term "writing" should be the same as in Section 178 of the Copyright, Designs and Patent Act. The Law Society still believes this to be the appropriate approach in order to avoid unnecessary duplication. Section 178 states that:

> "writing includes any form of notation or code, whether by hand or otherwise, and regardless of the method by which, or medium in or on which, it is recorded".

There will no doubt be cases where such a provision will be unsuitable, possible examples being cheques and bills of lading. It must be possible to exclude such cases by secondary legislation, exercisable say during two years from the coming into force of the Act, in cases where the DTI has been satisfied by the appropriate Minister that exclusion is necessary. This would be possible for a limited range of purposes such as consumer protection or the prevention of fraud.

Such an approach would demonstrate real commitment by the Government to the implementation of electronic commerce, and induce real urgency in Government departments required to identify cases requiring exclusion, as well as ensuring control of the process by the DTI. It is an approach consistent with that adopted by the draft European Electronic Commerce Directive.

If the Government retains power to impose conditions on the use of electronic communications and electronic writing and signatures in dealings between citizens and Government, it must ensure that electronic transactions are not imposed barriers or hindrances which are not applied to paper dealings. In particular, powers to legislate by statutory instrument should expressly provide that no electronic signature may be required to be certified by a third party in any case where a paper signature is not presently required to be authenticated in a corresponding way.

PART III INVESTIGATION OF PROTECTED ELECTRONIC DATA

As stated in the introduction to this response, the Law Society considers that law enforcement access issues should be addressed in a separate Bill. It has the following comments on the main law enforcement provisions of the Bill.

1. Proposed Structure of Accountability

The Government has indicated that the draft Bill does not affect safeguards in existing legislation and that it does not create any new powers for law enforcement agencies. The stated intention of the draft Bill is merely to allow law enforcement agencies to use existing powers effectively when they are faced with new technology.

However, the nature of the powers actually conferred on law enforcement agencies by the Bill, go beyond existing powers because the nature of the evidence obtained in electronic communications is different from evidence obtained in traditional communications. Providing fingerprints, DNA samples or

producing documentary evidence is not comparable to the disclosure of a key. The latter could, potentially, enable access to a wide variety of materials that may be confidential, legally privileged or have nothing to do with the investigation.

The Law Society appreciates that law enforcement agencies are anxious to tackle cyber crime and electronic communications between criminals, in particular because there is currently no legislation which can force a suspect to provide a key or code to decrypt a document. But this has to be balanced against the probability that creating direct or indirect control mechanisms for law enforcement agencies will drive electronic commerce users away from the UK.

E-commerce should not be hampered by law enforcement concerns. On this issue the Society shares the views expressed by the Trade and Industry Committee in May of this year:

> " Until recently the Government intended to use legislation to control cryptography rather than [to] encourage electronic commerce (..) [the Committee] expects the Government to (..) devise a cryptography policy which is best for the UK as a whole rather than one which is geared towards satisfying law enforcement concerns at the expense of Britain's economic competitiveness"

2. Proposed Safeguards

The safeguard structure proposed by the draft Bill is very similar to the one put forward in the Police Act 1996 and, although the Law Society recognises that the Government has tried to address concerns expressed about the Bill in 1996[4], a number of issues remain unresolved.

Of overarching concern is the excessive interference of the executive. In order for the system to be viewed as fair and trustworthy, law enforcement access to electronic communications has to remain under the sole control of the judiciary. At whatever level, the Bill must avoid Government intervention.

Schedule 1 to the draft Bill states that a warrant may be issued " by the Secretary of State or a person holding high judicial office". The schedule simply says that warrants authorising access to communications *may* be issued by a judge but the rest of the draft Bill does not mention this possibility at all. Maintaining sole Government control in this way is bound to damage both consumer confidence in and the credibility of the UK e-commerce market.

Requiring judicial authorisation for access electronic communications is surely a reasonable concept In December 1996, JUSTICE[5] produced a briefing for the Police Bill which focussed on intrusive surveillance in various common law countries (USA, Australia, New Zealand, Canada) and in civil law countries (The Netherlands, Germany, France, Germany). In all the jurisdictions surveyed, judicial authorisation is required for lawfully interception of communications and for the use of electronic surveillance devices. Warrants are issued by judges or magistrates competent to hear cases of serious crime in first instance.

[4] Two measures offer some protection for the consumer: 1) It is possible to introduce an appeal to the Tribunal's final determination. It is regrettable, however, that the appeal will only be possible on a question of law and with the leave of the Tribunal. If the Tribunal refuses, the leave of the appropriate court will be sought. 2) Procedure rules for the Tribunal will only be implemented once each House of Parliament has given its approval.

[5] British Section of the Commission of Jurists

To avoid the risk of "judicial rubberstamping" (the automatic delivery of warrants when these are requested), the New Zealand Supreme Court jurisprudence specifically requires judges to scrutinise cases by applying to strict standards.

In previous legislation governing intrusive interception of communications, the UK itself provided judicial safeguards. Police powers of entry, search and seizure (provided for at Section 8 of the Police and Criminal Evidence Act 1984 (PACE)), for example, are usually exercisable only with the authority of a warrant from a magistrate or a production order or warrant issued by a circuit judge (Schedule 1 and Code B of the 1984 Act).

As LIBERTY[6] emphasised in its *Briefing on the Police Bill 1996* in November 1996, failure to provide proper judicial safeguards will mean that the legislation "is likely to breach the requirements for independent scrutiny laid down by the European Convention on Human Rights".

The Law Society's proposals for judicial supervision of the e-commerce market are outlined in the conclusion to this response.

3. Key Components of the structure of accountability

The key accountability structure in the draft Bill is based on a Commissioner and a Tribunal. The Commissioner holds, or has held, a high judicial office his/her role will consist in supervising the Secretary of State when exercising the powers conferred to him/her by this Bill. He/she will also give assistance to a complaints Tribunal[7]. The Tribunal created by the draft Bill hears complaints against intrusive interception of communications.

The Prime Minister and the Secretary of State have a very prominent role in the work carried out by the Commissioner and Tribunal. Their interventions are such, that the proposed supervision mechanisms often appear to be mere extensions of governmental powers.

1. Commissioner

- the Prime Minister appoints the Commissioner to supervise the exercise of the powers conferred to Secretary of State by the Bill;
- the Commissioner presents an annual report to the Prime Minister on the work he carries out under the Bill;
- the Commissioner is *consulted* by the Prime Minister on matters which could be excluded form the report laid down before each House of Parliament. The Prime Minister is entitled to exclude a matter from these reports if he finds they will be prejudicial to the public interest in the following circumstances:

  - to national security;
  - the prevention or detection of serious crime;
  - the economic well-being of the United Kingdom; or
  - the continued discharge of the functions of any intelligence agency.

The Law Society is concerned that no specific criteria are put forward to suggest when it is proper for the Prime Minster to decide that these conditions have been met. Given the scope of the conditions, it

[6] Formerly the National Council for Civil Liberties.
[7] Section 18, Part III, draft Bill on Electronic Communications, 27 July 1999.

is likely that the Prime Minister will be able to exclude a whole range of measures without being held accountable in any way.

2. The Tribunal

- Schedule 2 of the draft Bill states that rules of procedure for the Tribunal are set out by the Secretary of State;
- the Secretary of State is authorised, amongst other, to decide that the Tribunal is not required to justify its decisions (Schedule 2 Paragraph 3 (3);
- the Secretary if State can also decide that the Tribunal may hold proceedings in the absence of the person concerned by the proceedings, including the complainant and any legal representative appointed by him (Schedule 2 Paragraph 3 (3) (b)).

Schedule I[8] of the draft Bill indicates that, when the Secretary of State drafts rules of procedure for

the Tribunal, no information is to be disclosed:

> " to an extent, or in a manner, that is contrary to national security, the prevention or detection of serious crime, the economic well-being of the United Kingdom or the continued discharge of the functions of any intelligence agency.

The above public interest considerations are, of course, the same as those mentioned in provisions relative to the Commissioner. The risk of lack of accountability is the same also.

Two further provisions demonstrate the intimate link between the Bill's proposed structure of accountability and the executive branch of Government. The first is that the Secretary of State has been given the task of ensuring that all salaries and expenses of the Tribunal are paid. The second is that not a single complaint has been upheld by existing (and similar) tribunals[9] so far. It is therefore reasonable to doubt whether the Tribunal put forward by the Bill will be any more effective.

4. Specific provisions relating to law enforcement access (Part III)

1. Disclosing plaintext or a key

A notice allowing access to encrypted material in a comprehensible, or plaintext, form is already required by existing legislation[10]. Duplicating existing legislation in this way is unnecessary and confusing.

On the issue of disclosing a key, there must be greater clarity on: a) the conditions which must be satisfied in order for a key to be requested and, b) the safeguards which will ensure that law enforcement agencies are held accountable if and when they venture beyond the limits of a notice authorising access to a key.

Many provisions of the draft Bill on electronic communications still lack the level of clarity or practicality that would instil consumer confidence. Below are examples, which illustrate this concern.

Clause 10 (3): provides that a notice requiring a key:

[8] Schedule 2 Paragraph 3 (5) (b)
[9] Set up by legislation on intrusive surveillance: Interception of Communications Act 1985, the Security Service Act 1989, the Secret Intelligence Act and the Intelligence Services Act 1994.
[10] Police and Criminal Evidence Act 1984 Paragraphs 5 (a) and (b).

" may take such form and be given in such a manner as the person giving it thinks fit".

No criteria are suggested to assess when a person giving a notice can choose a form and a manner which he/she "thinks fit". There is also no mention of what conditions justify the renewal of a warrant.

Clause 10 (5): provides that:

" a notice under this section shall not require the disclosure of any key which-

(a) is intended to be used for the purpose of electronic signatures; and
(b) has not in fact been used for any other purpose".

Several systems allow one key to operate both encryption and electronic signature services. Section 10 (5) appears to assume that there is necessarily a separate key for each procedure. Under the draft Bill, a key which can operate both signature and encryption functions need only have been used once to decrypt material for it to cease to be just a signature key. This being the case, law enforcement agencies will have the right to request that key be disclosed.

Clause 11 (3): provides that a person, who is required to disclose a key by a written notice may, instead, provide the data in an intelligible form, unless the person who gave the authorisation to require the disclosure, or a person entitled to give such authorisation, has specified that only the disclosure of a key itself is sufficient.

There do not appear to be any criteria in the draft Bill, which explain when a decision to require " the disclosure of a key itself is sufficient" is justified, leaving the point to pure executive discretion.

Clause 12 (1): provides that a person is guilty of an offence is he/she fails to comply with a notice to disclose key protected information unless the person shows (Clause 12 (1) (a)):

" 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"

The above clause requires a person to prove "that he/she did not have a key" at any given time. It is not possible to prove a negative. The clause may therefore be contrary to Article 6 of the European Convention on Human Rights (which provides that everyone charged with a criminal offence shall be presumed innocent until proven guilty according to law) The absence of any obligation imposed on the prosecution to show the addressee of the notice ever had the key, only makes a breach of the Convention more certain.

Clause 12 (4): also states that:

" (..) a person shall have a defence under subsection (2) or (3) only if he also shows that it was not reasonably practical for him to comply with the requirement in the manner allowed by that section".

The draft Bill does not suggest criteria that could be used to assess if a situation is or is not "reasonably practical". Such criteria must be detailed to clarify the potential obligations of consumers.

Clause 13 (3) (a): provides that:

" In proceedings against any person for an offence under [Clause 13] it shall be a defence for that person to show 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"

The Law Society would suspect that many IT systems are likely to have such a software and, that, at any rate it is more than likely that communications between criminals will use reasonably sophisticated IT systems. If this is the case, the defence offered at Clause 13 (3) (a) might have a considerably wider scope than was originally intended.

2. Tipping-off

The Law Society is pleased to see that, under Clause 13 (4) (a) and 13 (5) of the draft Bill, a legal adviser cannot be held accountable for tipping-off information on a notice given under the Bill. In providing these clauses, the Government appears to offer some acknowledgement that a solicitor has a duty of full disclosure to his/her client, particularly if the information is relevant to the legal advice which is being given.

It is unfortunate, however, that Clause 12 does not protect solicitors from having to provide a key to access encrypted communications (some of which may well be privileged). In accordance with the Society's previous response to the DTI and the Government's stated intention to abide by human rights standards, it is strongly suggested that the Bill incorporate a *general* defence for solicitors against the offence of tipping-off, and a general right both to refuse to disclose privileged material (whether encrypted or not) and to deliver plaintext instead of a key in any case where the key may provide access to privileged material.

III. CONCLUSIONS AND RECOMMENDATIONS

- The Law Society urges the Government to **limit the scope of the draft Bill to the promotion of the UK e-commerce market.** Law enforcement should be addressed in a separate and uniform piece of legislation covering general access to and admissibility of all communications, of whatever kind. Law enforcement access to electronic communications could, for instance, be provided for in the Police and Criminal Evidence Act (PACE), which regulates the interception of traditional documents, or in amendments to the Interception of Communications Act 1985, which is currently being reviewed.

- In the interest of consumer confidence, the Society suggests that the **Government intervene as little as possible in the e-commerce market**. The Law Society's preferred option for law enforcement access, is to replace the proposed Commissioner and Tribunal with a purely judicial

control mechanism. This should be the case even if a party has consented to intrusive surveillance ("participant monitoring").

Whatever regimes provide for law enforcement access it must take into account of the European Convention on Human Rights

- Finally, in order to abide by the Government's principle of providing **technology neutral legislation**, provisions covering the licensing regime of cryptography service providers (Part I of the draft Bill) should be changed. It should be made clearer that registration of cryptography service providers is entirely voluntary and, therefore, that a registered service provider cannot be considered more trustworthy than a non-registered provider. It is up to the market, not the law, to decide whether a specific business model is appropriate and necessary.