RESEARCH PAPER 99/100
8 DECEMBER 1999

The *Electronic Communications Bill*

(revised edition)

Bill 4 of 1999-2000

This Bill aims to encourage the use of electronic commerce by legislating on some points relating to suppliers of cryptography services and to electronic signatures. It also provides for a revision in the procedure for modification of licences for telecommunications operators. It applies to the whole of the United Kingdom. This paper has been updated to include the Second Reading Debate and replaces Research Paper 99/92.

Christopher Barclay

SCIENCE AND ENVIRONMENT SECTION

HOUSE OF COMMONS LIBRARY

Recent Library Research Papers include:

99/85	The Procedural Consequences of Devolution	20.10.99
99/86	Economic Indicators	01.11.99
99/87	The prospects for Russia	08.11.99
99/88	The *House of Lords Bill* – Lords Amendments [Bill 156 of 1998-99]	09.11.99
99/89	Family Leave	11.11.99
99/90	Unemployment by Constituency – October 1999	17.11.99
99/91	Millennium Trade Talks – Food and Agriculture Issues	19.11.99
99/92	The *Electronic Communications Bill* [Bill 4 of 1999-2000]	24.11.99
99/93	The Climate Change Levy	24.11.99
99/94	The *Representation of the People Bill* [Bill 2 of 1999-2000]	25.11.99
99/95	By-elections since the 1997 general election	29.11.99
99/96	Economic Indicators	01.12.99
99/97	The *Government Resources and Accounts Bill* [Bill 3 of 1999-2000]	30.11.99
99/98	The *Freedom of Information Bill* [Bill 5 of 1999-2000]	03.12.99
99/99	The *Freedom of Information Bill*: Data Protection Issues [Bill 5 of 1999-2000]	03.12.99

Research Papers are available as PDF files:

- *to members of the general public on the Parliamentary web site, URL:* ***http://www.parliament.uk***
- *within Parliament to users of the Parliamentary Intranet, URL:* ***http://hcl1.hclibrary.parliament.u****k*

Library Research Papers are compiled for the benefit of Members of Parliament and their personal staff. Authors are available to discuss the contents of these papers with Members and their staff but cannot advise members of the general public.

Users of the printed version of these papers will find a pre-addressed response form at the end of the text.

ISSN 1368-8456

Summary of main points

- Electronic Commerce is spreading very fast, and presenting considerable problems to legislators.
- The Electronic Commerce Bill is the result of consultation with the industry following on earlier proposals.
- Some of the original proposals – particularly those connected to encryption – have been dropped from the Bill and may appear in some form in other legislation.
- The Bill provides for a voluntary system of registration of suppliers of cryptography services.
- The Bill makes provisions to facilitate the use of electronic signatures.
- The Bill amends to procedure for modification of licences for telecommunications operators in order to allow for the fact that there are now large numbers of such operators.

CONTENTS

I Background to the Electronic Communications Bill

A. The Growth of Electronic Commerce

a. Worldwide Growth of Electronic Commerce

Predictions regarding Internet growth are uncertain. It is estimated that the number of users[1] on line worldwide will rise from 179 million at present to some 250 million in 2000 and to 350 million by 2005. This should be compared to an estimated 130,000 users in 1990. By 2003 one in three households in Europe- 43 million - will be on line.[2] Germany is currently the largest Internet market in Europe, followed by the UK and then the Netherlands. According to Datamonitor, in Europe today almost 2.2 million businesses are using the Internet. By 2004, there will be 5.4 million, which means that two thirds of European businesses will have access.[3]

The predictions for internet usage suggest impressive, but steady, growth. The predictions for electronic commerce are quite different, suggesting dramatic growth from a low base, even though all such figures, even about the current position, are necessarily uncertain. It has been estimated that global electronic commerce (or e-commerce) was worth $12 billion in February 1999, and will grow to $ 350-500 billion by 2002 and to $1 trillion by 2003-05[4] with huge potential growth in the area of financial services and professional services such as accountancy and consulting.[5] Presumably, little progress can be made in electronic commerce until internet usage is widespread. At that point, however, it can spread extremely quickly.

The global market for E-commerce software will be worth $2 billion in 2002 with Europe making up almost half of this, catching up with America.

The Trade and Industry Select Committee produced a report on E-Commerce in July 1999, including some figures on its extent. The estimate of $43 bn for business to business electronic transactions in 1998 comes from evidence to the Committee from InterForum, while the lower figure quoted above came from evidence at the same time from the DTI.

---

1 Figures represent both adults and children who have accessed the Internet at least once during the 3 months prior to being surveyed, not just Internet Account holders

2 Datamonitor Press Release, 7 December 1998

3 http://www.datamonitor.com

4 Trade and Industry Committee, *"Building Confidence in Electronic Commerce": the Government's proposals*, HC 187 1998-99, p xii, 12 May 1999

5 "World Trade: WTO weighs duty free trade on the Internet", *Financial Times*, 20 February 1998

> 6. We indicated in our first Report on electronic commerce that we consider three broad sets of transactions, which rely directly on computers, to comprise electronic commerce, namely:
>
> - business to consumer transactions
> - business to business transactions
> - citizen to Government transactions.
>
> Most electronic commerce is conducted between businesses. In 1998 it is estimated that $43 billion of business to business electronic commerce was transacted worldwide and it is currently predicted that this will increase to $300 billion by 2002. Much of this trade is well-established, making use of closed networks such as the EDI system rather than open-networks such as the internet. Electronic commerce between businesses and consumers is currently less significant — perhaps worth $7 billion worldwide in 1998 — but is growing rapidly and is expected to total as much as $80 billion in 2002. Business to consumer electronic commerce has been the source of considerable comment and speculation, much of it exaggerated. Citizen to Government electronic commerce encompasses a wide range of transactions, from Government procurement to the electronic submission of tax returns, electronic voting and the communication of information between citizens and Government departments… In the US we were made aware of a fourth form of electronic commerce, consumer to consumer transactions, including on-line auctions facilitated by firms such as eBay.[6]

b. The position in the UK and parts of Europe

The latest NOP Internet User Profile Survey found that 12.7 million people currently have Internet access in Britain and that the Internet is attracting 10,900 new adult users in Britain every day.[7] Some 10.6 million adults accessed the Internet at least once during 1998, a 50% increase from 1997. This growth may have been encouraged by the introduction of free connections such as Dixon's Freeserve.

However, a survey in the summer of 1999 suggests that the UK is making more use of the Internet than was previously thought.

> According to a major new survey, 40% of adults in the UK now have some way of accessing the internet and over a quarter of UK adults used the net in the last month. Young men and women, aged 16 to 24, not surprisingly are leading the way into the digital future, with nearly 70% online. But significant numbers of older people are also embracing the net - over 50% of men aged 35 to 49, and 40% of women in same age group. The over 50s also have a net presence - 25% of men and 16% of women… [8]

---

6 Trade & Industry Committee, *Electronic Commerce*, 15 July 1999, HC 648 1998-99

7 NOP Research Group, March 1999

8 "Net catches the UK", http://news.bbc.co.uk, 26 October 1999

E-commerce in the UK is still very much at an early stage. A 1998 survey by NOP Research Group showed that only 13% of UK companies were using the Internet for on-line sales. The main reason for UK companies to have a web site was found to be for advertising and marketing (77%).[9]

In Europe, public purchasing amounts to 11% of European GDP. The European Commission has set a target of 25% of public procurement transactions to take place electronically by 2003 to encourage electronic commerce.[10] With the same aim, the UK Government has announced targets of procuring 90% (by volume) of routine goods electronically by 2000/2001 and making 25% of Government services available on-line by 2001.[11] Datamonitor predict that by the end of 1999, consumers in Germany, the UK and France will spend $290 million, $170 million and $85 million respectively shopping online. The European market for online shopping is expected to grow to $8.6 billion by 2003.[12]

At the moment the only access to on-line shopping is via the Internet and so the cost of installing a PC at home may be a barrier to this. Mobile phones and set-top boxes, which are much cheaper and already widespread, lay open the possibility of more diverse platforms for e commerce. These products already use smart cards, which could be made capable of payments. Datamonitor therefore expects that by 2003, $623 million of European online spend will be via e-commerce smart cards.[13]

c. The importance of E-Commerce

Datamonitor considers that companies will increasingly be left with little choice but to invest in E-commerce. Whereas business to consumer (B2C) E-commerce has dominated so far, and B2C software accounted for 41% of the E-commerce software market in 1997, business to business (B2B) E-commerce software will account for 78% of total revenues in 2002. This is because as trading communities form those left out will be at a disadvantage.[14]

---

9 DTI, *Moving into the information age: International benchmarking study 1998*, April 1998

10 DTI Press Notice P/98/155, *Net benefit: Barbara Roche sets out Britain's electronic commerce agenda*, 6 October 1998

11 ibid

12 Datamonitor Press Notice, *Mobile phones and set-top boxes to emerge as platforms for online-shopping*, 14 June 1999

13 ibid

14 Datamonitor Press Notice, *Europe will be the fastest growing market for e-commerce software to 2002*, 29 June 1999

It is clear already that E-Commerce is very important to business, but at the moment its importance is confined to particular areas. Marketing is the obvious area where a firm without E-Commerce is likely to lose out, even if the actual orders are not made electronically. Thus, a potential customer may use the internet to find out about suppliers even if he then discusses with them in more detail in person or by letter before completing a transaction. For many goods, it is now possible to buy on the internet and that possibility introduces international competition from the start. Indeed, when you first contact a website, it is often not obvious whether the company involved in based in the UK or the USA, or anywhere else.

d. The role of legislation

The predicted explosive growth of e-commerce and the huge commercial opportunity pose considerable problems for legislators. Business on the internet is likely to be internationally mobile, so too restrictive a legislative framework will drive it away to other host countries. In addition, restrictions may prevent entrepreneurs with new ideas to create wealth via new ideas and new businesses from flourishing.

At the moment, E-Commerce is developing so fast that it is difficult for legislators to keep up. There are many issues to be decided. It would be easiest for companies if all countries had the same law relating to E-Commerce transactions, but that would probably take several years to negotiate and ratify as an international treaty, leaving the intermediate period without suitable legal guidance. Governments are therefore trying to legislate to deal with immediate problems, such as the validity of electronic signatures, but without being so prescriptive as to inhibit the growth of this new commerce. They fear, of course, that if the legislation is too prescriptive, then the commerce will simply move to a less strict regime.

In some ways it is tempting to avoid legislation altogether, until the time when the whole world can agree on adopting the same system. However, that option would create a further set of problems. International agreements are normally only reached after years of negotiation, and are then followed by years more before ratification by enough countries brings the agreement into force. In the meantime, there would be a legislative vacuum, which might mean that British companies would become involved in costly litigation.

In addition, there are several areas related to electronic commerce, but outside the scope of this Bill, where legislation may be required, including both law enforcement and taxation. The current Bill, however, has been kept small so as to concentrate upon the topics that are considered necessary to make electronic commerce flourish, rather than to cover all the possible areas.

B. Earlier Government Proposals

For several years this Government and its predecessor have been trying to find the appropriate legal framework for e-commerce. Consultation in March 1997 by the Conservative Government was followed by a statement a year after the election:

> **Dr. Ladyman:** To ask the President of the Board of Trade how the Government intends to encourage electronic commerce; and if she will make a statement.
>
> **Mrs. Roche:** The Information Age strategy launched by the Prime Minister on 16 April demonstrates the Government's commitment to electronic commerce. Electronic commerce is crucial to the future prosperity of our economy and to the competitive position of our industries, and the UK is well placed to play a leading role. Building on the success of the Programme for Business, the Government are now putting in place the policy and legal framework in which electronic commerce can flourish. From schools to high finance in the City the Government are committed to ensuring everyone benefits from advanced electronic communications.
>
> It is also important to make electronic commerce more secure. Users cannot afford to let the information they transmit across the Internet (or any other network) be compromised. They must have confidence that both the integrity and confidentiality of their information will be protected. At the same time, users must be able to trust both the technologies which allow such security and the commercial organisations providing it. To that end, I am announcing today proposals for legislation to introduce voluntary licensing arrangements for bodies offering cryptographic services to the public to ensure that minimum standards of quality and service are met. They will apply to both Certification Authorities (providing electronic signature services) and other bodies providing encryption services. The arrangements will set minimum technical and competence standards for bodies that wish to seek licences. The legislation will also enable users to place greater reliance on digital signatures, through a presumption of legal recognition for those signature generated by licensed Certification Authorities. Fuller details of this policy are set out in a Statement which is being lodged in the Libraries of both Houses. (DTI, Secure *Electronic Commerce Statement*, April 1998, Deposited Paper 98/298)
>
> It is not, however, in the interests of business or the public for criminals and terrorists to be able to exploit these new technologies to disguise or conceal their activities. To meet these concerns, the Government will also introduce legislation making provision for law enforcement agencies to gain legal access, under a properly authorised warrant and on a case by case basis, to encryption keys or other information protecting the secrecy of stored or transmitted information. The purpose of these new powers will be to maintain the effectiveness of the existing legislation designed to protect the public from crime and terrorism.[15]

---

[15] HC Deb 27 April 1998 cc 26-27W

The latter half of the statement remains controversial, with a clear difference of view between those wishing to expand the use e-commerce and the law enforcement agencies who fear that their powers to detect criminal activity might, in practice, be reduced.

The Government made two sets of proposals on e-commerce in 1999 before the publication of the current Bill, with the changes marked by leaving out proposals that did not suit those who use E-commerce. The main change is the dropping of the part of the bill relating to encryption, but the part on electronic signatures has also been changed. The changes are explained in section II and section IIIB respectively. The original proposals came in *Building Confidence in Electronic Commerce: A Consultation Document*, in March 1999.[16] Comment on these proposals included a report by the Trade and Industry Select Committee.[17] There was another White Paper in July 1999, called *Promoting Electronic Commerce,* which contained a draft Bill.[18] There was also a further report in July 1999 from the Select Committee, *Electronic Commerce*.[19]

The Trade and Industry Committee then produced a report specifically on the draft Bill.[20] This current paper does not repeat the detailed arguments in the latest Select Committee Report, since it is easier to read the original report.

C. The aims of the current Bill

The DTI Press Notice launching the Bill described its objectives:

> Ms Hewitt said:
> "This historic Bill will help make the UK the best place in the world to do electronic business. Britain led the world in the first industrial revolution. Now we are determined to be winners in the new knowledge economy revolution. This Government is creating the conditions in which UK businesses can thrive and where the UK becomes first choice for investors.
>
> "Many of our laws are hundreds of years old. They were written for the days of pen and paper. Today's businesses operate with e-mail and digital signatures. We must modernise our laws if we are to compete in the electronic market-place.
>
> "We are determined to get e-commerce law right and get it in fast. That is why we are introducing this Bill in the same week as the Queen's Speech. We are on course to meet our original target for Royal Assent by April 2000 making this one of the UK's first 21st century laws."

---

16 DTI, *Our Competitive Future: Building the Knowledge Driven Economy*, December 1998

17 Trade and Industry Committee, *"Building Confidence in Electronic Commerce": the Government's Proposals*, HC 187 1998-99

18 DTI, *Promoting Electronic Commerce*, July 1999, Cm 4417

19 Trade and Industry Committee, *Electronic Commerce*, 15 July 1999, HC 648 1998-99

20 Trade and Industry Committee, *Draft Electronic Communications Bill*, 26 October 1999, HC 862 1998-99

Under the legislation:

- electronic signatures will be given explicit legal recognition by the courts for the first time, giving people a secure electronic alternative to paper;

- obstacles in existing laws which insist on the use of paper will be swept away wherever it makes sense to give people the electronic option;

- a 'kitemarked' self-regulatory approvals scheme will be established to ensure minimum standards of quality and service. People will be able to check who has sent an electronic message, ensure it has not been tampered with and that no-one else has read it on the way;

- if the self-regulatory scheme works, there will be no need to set up a statutory scheme. Only if self-regulation failed would the Government establish a statutory scheme which would also still be voluntary. This part of the Bill will be subject to a 'Sunset Clause'. If a statutory scheme has not been set up within five years then the Government's power to set one up would lapse.

Following two extensive consultations on the draft Bill with business and the IT industry the Government also announced that:

- mandatory key escrow has been explicitly ruled out in the Bill;

- important law enforcement powers have been moved from this Bill to the Home Office 'Investigatory Powers Bill' to be debated alongside a comprehensive updating of similar legislation.

Home Office Minister Charles Clarke said:

"Encryption is a double-edged sword - both vital to the e-commerce revolution and at the same time a deadly weapon in the hands of criminals. Paedophiles, drug traffickers and terrorists are already using encryption to try and evade justice. This cannot be allowed to continue. As encryption becomes more readily available and easier to use, the need to modernise police powers to enable them to read the material they can already lawfully get access to becomes ever more urgent.

"That is why the Government will provide law enforcement agencies with new powers to access decryption keys and the plain text of lawfully obtained material under properly authorised procedures containing strong safeguards. We have listened and reflected on how best to update the statute book and have decided to take the measure forward this session in the Investigatory Powers Bill instead of the Electronic Communications Bill."[21]

---

[21] DTI Press Release P/99/938, *Era of Electronic Signatures Dawns - Hewitt*, 19 November 1999

II Encryption

Encryption is one of the key problems for legislators. On the one hand, it is hard to imagine an extension of e-commerce, particularly for business to business transactions, without the use of encryption. On the other hand, many Governments believe that they need to have some control over encryption to prevent its misuse. The original proposals - for key escrow - have been dropped, because the industry argued that the Government was taking too much power to read coded information. The term "key escrow" describes a system in which the person who encrypts data has to leave the key with a third party. A modified version was in the draft Bill but is not in the current Bill. Some version is expected in an Investigatory Powers Bill, a Home Office Bill expected in early 2000. At this stage, we do not know whether the moving of the proposals from one bill to another represents a change in policy or a mere rearrangement of the legislative programme.

Building Confidence in Electronic Commerce explained why encryption was considered to pose a serious threat to law enforcement.

> 49 A number of recent investigations into a variety of serious criminal offences in the UK have been hampered by the discovery that material which might otherwise assist the investigation, or be used in evidence, has been encrypted. The problem is increasing. Law enforcement agencies often try to "crack" the encryption key. Although this is occasionally possible after considerable effort and expense, it is likely to become increasingly difficult – if not impossible – as the technology develops.

It then gives examples:

- A case of attempted murder and sexual assault;
- Numerous cases of paedophiles using encryption;
- The Serious Fraud Office estimated that in approximately 50% of its cases, some form of encryption was encountered;
- Commercial interests faced a range of potential threats from improper use of encryption, including corporate espionage, insider theft, and attempts at extortion of money by placing enciphered viruses into computer systems.
- Terrorists were using encryption as a means of concealing their activities.

Building Confidence in Electronic Commerce continued:

> 64 The Government proposes to establish a power to require any person, upon service of a written notice, to produce specified material in a comprehensible form or to disclose relevant material (e.g. an encryption key) necessary for that purpose. The ability to serve a written notice will be ancillary to existing statutory powers such as those contained in the *Interception of Communications Act 1985* and the *Police and Criminal Evidence Act 1984*. This means it will apply only to material which itself has been, or is being, obtained lawfully.

> 65 The new power will not make access to any encrypted communications or data lawful if it would otherwise be unlawful. For example, it is an offence to intercept communications on a UK public telecommunications network without a warrant issued by a Secretary of State. It will not be possible to obtain the Secretary of State's authorisation for access to encryption keys to decrypt unlawfully intercepted material.

Already, in *Building Confidence in Electronic Commerce*, the idea of tackling key escrow separately is suggested:

> 82 The Government remains keen to promote key escrow and their party key recovery technologies. However, the electronic commerce market is developing quickly. Industry has expressed serious concerns that imposing a requirement for key escrow or third party key recovery as part of the licensing scheme would place unreasonable constraints on the development of electronic commerce in the UK. That is why the Government is consulting on the basis that the licensing scheme will not impose the requirement that Trust Service providers (ie cryptography service providers) providing confidentiality services should have to provide for law enforcement access to keys in this manner.

In other words, the Government wanted to facilitate electronic commerce but was persuaded of the need for law enforcement agencies to read encrypted correspondence where necessary.

The draft Bill in *Promoting Electronic Commerce* contains a power to require disclosure of key in Clauses 10 to 13. The way that the Clauses would have worked is explained in the explanatory passages in this White Paper:

> Clause 10: Power to require disclosure of key
> This Clause sets out the conditions under which notices can be served requiring disclosure of a key necessary to make lawfully obtained protected information intelligible. This Clause introduces a power to enable properly authorised persons (such as members of the law enforcement, security and intelligence agencies) to serve written notices on individuals or bodies requiring the surrender of information (such as a decryption key) to enable them to understand (essentially make intelligible) protected material which they legally hold or are likely to. By way of illustration, this could include material:
>
> - seized under a judicial warrant (e.g. under the Police and Criminal Evidence Act 1984);
> - intercepted under a warrant personally authorised by the secretary of state under the interception of Communications Act 1985;
> - lawfully obtained by an agency under their statutory powers but not under a warrant (e.g. section 18 of the police and Criminal Evidence Act – on entry and search after arrest); or
> - which has lawfully come into the possession of an agency but not by use of statutory powers (e.g. material which has been voluntarily handed over).

> The service of a written notice will need to be authorised by, for example, the Secretary of State, a judge, or a senior police officer, depending on the powers under which the protected material was or is likely to be obtained…
>
> Clause 11: Disclosure of information in place of key
> This Clause provides that a person required by a written notice to disclose a key 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 the key itself is sufficient…
>
> Clause 12: Failure to comply with a notice
> This Clause makes it an offence to fail to comply with a notice given under Clause 10…
>
> Clause 13: Tipping-off
> This Clause creates a new offence where the recipient of a notice, or a person that becomes aware of it, tips off another that a notice has been served or reveals its contents.[22]

However, these proposals were controversial and rather unpopular within the e-commerce world. To some extent that might be explained by the fact that the industry is interested in extending commerce and not in catching criminals. However, concern about the proposed powers went beyond that. The human rights organisation *Justice* obtained a legal opinion from Jack Beatson QC and Tim Eicke, arguing that this part of the draft Bill would not have complied with the *Human Rights Act 1998*.[23] The question of compliance with the Human Rights Act may be important in the context of the Investigatory Powers Bill, but the arguments should not be relevant in the current Bill, because of the removal of the encryption part. The lawyers argued that the proposed Government power to read encrypted e-mails conflicted with Article 8 of the European Convention on Human Rights.

On the other hand, the Trade and Industry Select Committee was not alarmed by the proposed powers, and rejected the view that they represented a "major assault on our rights".[24]

---

22 DTI, *Promoting Electronic Commerce*, July 1999, Cm 4417, pp 23-25

23 www.fipr.org/ecomm99/ecommaud.html

24 Trade and Industry Committee, *Draft Electronic Communications Bill*, HC 862 1998-99, p xxviii

III The Bill

A. The current Bill and the Draft Bill

This Bill follows a draft Bill published in July 1999.[25] Parts I and II for the new bill correspond closely to the draft Bill. Part III of the draft bill, "Investigation of protected electronic data", has been withdrawn form the Bill and in some form will apparently form part of an Investigatory Powers Bill to be published in the year 2000. Part III of the Bill corresponds to part IV of the draft Bill.

The Bill covers both cryptography and electronic signatures, but these are closely related, as the Explanatory notes point out. Public key cryptography, which involves the use of one key for "locking" a document and another for "unlocking" it, can be used for both purposes. The Government's dilemma is to legislate so as to facilitate the use of the technology for legitimate commerce, but to prevent the same technology being used for the facilitation of crime.

The Bill was accompanied by Explanatory Notes produced by the Government, which give a good explanation of the Bill. This part of the paper is designed to read in conjunction with them.

B. Part I of the Bill and Clause 13

This part covers the regulation of cryptography service providers, and reflects the Government's compromise between the needs of the industry and those of crime prevention. The Government's plan is to set up a statutory scheme of registration of cryptography providers only if self-regulation by the industry does not work.[26] One of the questions raised by this approach is how one would judge whether self-regulation "does not work".

The original proposals, in March 1997, would have required that all companies offering cryptographic services to UK customers would require a licence. As a condition for that licence, cryptography service providers would have to hold copies of customers' private encryption keys and to provide law enforcement agencies with access to such keys in certain circumstances. This was the "key escrow" proposal. The Press Notice accompanying the Bill notes that the Government rejected this policy earlier this year because it would have imposed unfair burdens on law abiding citizens but it would have been possible for criminals to evade. It adds that "mandatory key escrow has been ruled out explicitly in the Bill".[27]

---

25 DTI, *Promoting Electronic Commerce*, July 1999, Cm 4417

26 DTI, *Electronic Communications Bill: explanatory notes*, p 16

27 DTI Press Notice P/99/938, *Era of Electronic Signatures dawns - Hewitt*, 19 November 1999

Part I of the current Bill is very close of Part I of the Draft Bill, but it contains a passage to limit the scope of the information that can be required as a condition for registration. It is difficult to assess how the proposals of Part I would work as it is largely a framework to be filled by secondary legislation. It allows the Secretary of State to establish a licensing regime, but it also allows him (in Clause 3) to delegate the approval function. Clause 2 is drafted so as to allow delegation, and Clause 3 explicitly allows the delegation. This would allow him to accept a scheme offered by the industry, but it would not compel him to do so.

However, the powers granted to the Secretary of State are not unlimited. In particular they would not allow her to prevent unlicensed companies from providing cryptography services. That would require further primary legislation, probably creating a criminal offence in this area. Therefore, even if the Secretary of State were to impose onerous conditions upon cryptography service providers – for example in terms of the requirements to provide information (Clause 2 (5)) it would remain open to cryptography service providers to choose not to be part of the licensing scheme. They might suffer commercial loss through lack of credibility by operating outside the scheme, but it would not be illegal.

Clause 2 (6) would limit the scope of the information that could be required. Since that sub-clause did not appear in the Draft Bill, it may be an attempt to deal with concerns raised in the consultation process. It reads as follows:

> Nothing in the arrangements shall authorise the imposition, by conditions contained in an approval, of any requirements for -
>
> (a) the provision of information, or
> (b) the maintenance of a procedure for handling complaints or disputes, in relation to any matter other than one appearing to the Secretary of State to be relevant to the matters mentioned in Subsection (3) (a) to (d).

The matters in Subsection (a) to (d) relate to the ability of the cryptography service provider to provide the service. In other words, Clause 2 (6) would appear to rule out the imposition by the Secretary of State of a requirement to provide information because the Secretary of State was interested in it – for example in any attempt to introduce key escrow by the backdoor.

This restriction fits in with the explicit rejection of key escrow in Clause 13 which states that the Act will not allow a Minister to impose a requirement on any person to deposit a key for electronic data with another person, apart from two exceptions unrelated tot he main issue.

After the publication of the draft Bill, fears remained in the industry that the proposals might allow the Government to use the licensing regime as a way of imposing conditions on the firms that would have allowed the government to read encrypted messages. The following summary of replies to the consultation exercise on part I of the draft Bill shows the fear clearly:

> 10. Most responses approved the ideas behind Part I, and were in favour of self-regulation. There was some concern that by taking reserve powers for a statutory scheme the Government is introducing uncertainty. A few took this to the extent of a call to drop Part I entirely ('trust the industry', or 'trust the market', or 'the approval of cryptography services is only marginally relevant to promoting electronic commerce'). Others wanted a quick decision by the Secretary of State, and/or criteria for judging the adequacy or otherwise of any industry schemes; however there was only one comment (favourable) on the criteria proposed in paragraph 28 of the consultation document.
>
> 11. There was much concern that, in the event that the reserve powers are invoked and a statutory scheme introduced, the Secretary of State's powers under secondary legislation are very wide and potentially incompatible with the desired 'light touch' approach to regulation in this area. For example it was said that he could 're-introduce key escrow by the back door', or demand disproportionate amounts of data to be disclosed, or delegate some of his powers to an inappropriate regulatory body. There was therefore a call for more limited or precise powers, and for a guarantee of adequate further consultation on the details before they are specified.[28]

The Trade and Industry Select Committee called for the Bill to exclude explicitly the use of key escrow as a criterion for accreditation under a statutory accreditation scheme, so the Bill appears to be in line with that recommendation.[29]

C. Part II of the Bill

This part deals with electronic signatures. Originally the Government intended to introduce, a system whereby licensed Certification Authorities would be in a position to offer certificates to support particular categories of electronic signatures reliable enough to be recognised as equivalent to written signatures:

> This will be done by creating, in statute, a rebuttable presumption that an electronic signature, meeting certain conditions, correctly identifies the signatory it purports to identify; and, where it purports to guarantee that the accompanying data has not been altered since signature, that it has not.[30]

However, that idea was not popular in the industry. For example, Microsoft welcomed the Draft Bill, by which time the idea of rebuttable presumption in favour of electronic signatures had already been dropped:

> The draft Bill provides that all electronic signatures are admissible into evidence and grants no particular category of electronic signature a rebuttable presumption of validity. Microsoft concurs completely with the Government's decision to

---

28 www.dti.gov.uk/cii/elec/billsumm.html (on the DTI website)

29 Trade and Industry Committee, *Draft Electronic Communications Bill*, HC 862 1998-99, p xxvii

30 DTI, *Building confidence in Electronic Commerce*, 5 March 1999, Deposited Paper 99/494, para 19

> extend the time-honoured treatment of signatures found at common law to the electronic realm: namely, that all electronic signatures are admissible in evidence, subject to proof of their reliability. A rebuttable presumption of validity for certain types of electronic signatures would have lessened consumer confidence in electronic commerce, imposed unnecessary costs on providers and users of electronic signature products, and upset existing legal rules and commercial practices. In particular, it would have distorted the market for electronic signatures by supplying an artificial incentive to use particular technologies or providers, regardless of whether they were best suited for the needs of the transaction. Such a presumption has never been a feature of handwritten signatures, and its introduction solely with respect to electronic signatures would have substantially altered existing legal doctrine and business practices.[31]

The DTI summary of replies to the Consultation Document, *Promoting Electronic Commerce*, describes the main views:

> 13. There was virtually unanimous approval for the intentions of Part II, but some doubt about its mechanisms. On electronic signatures, their specific application to data as well as communications was seen as essential.
>
> 14. Many significant players also wanted explicit statutory recognition to be given to electronic signatures as indicating the signer's approval of the signed data, or authority to act: clause 7 appears to establish only their admissibility as evidence of authenticity and integrity, and not their full legal recognition as signatures (as apparently intended in paragraph 9 of the explanatory notes). Indeed some felt that in conferring admissibility for limited purposes the Bill could discourage the natural development of the common law towards recognising electronic signatures more fully. Some respondents assumed that clause 7 does indeed provide for 'legal recognition of signatures', and welcomed it.
>
> 15. There were doubts about the definition of certification of an electronic signature: it was pointed out that technically what is normally certified is the public key of the purported signer together with their possession of the related private key and some degree of confidence in their identity.
>
> 16. As discussed in paragraph 8 above, there was much doubt about the effectiveness of clause 8's 'opt-in' approach. Ireland's model (and that of various other countries) providing for the general validity of electronic writing subject to defined 'carve-outs' (wills, marriages, land, etc) was often preferred.
>
> 17 There was concern over the uncertainty that 'opt-in' could produce and the likely prolonged timescale of its implementation; there was concern also that the wide nature of the proposed powers available to Ministers could lead to significant inconsistencies of detail and implementation. For both these reasons, strong and effective co-ordination by the Government was called for to set priorities and deadlines, to ensure coherence, and to preserve the overall aim of furthering electronic commerce. The non-application of clause 8 to Inland

---

31 Microsoft's Response to the Government's Consultation Document: *Promoting Electronic Commerce*, October 1999

> Revenue and HM Customs was also considered a potential source of inconsistencies.
>
> 18. There were varying views on the Parliamentary process proposed under 'opt-in', with some calling for positive approval for all orders or statutory instruments. The proposed 'positive for the first and negative thereafter' approach was seen as a reasonable compromise but, again, heavily dependent on strong co-ordination by the Government.[32]

As with Part I of the Bill, Part II also creates powers for making secondary legislation, in this case to devise an appropriate set of rules for electronic signatures. In this case the powers are granted to "the appropriate Minister" rather than to the Secretary of State for Trade and Industry. The reason for this is that many different pieces of legislation in different fields might have to be amended in order to deal with the different aspects of electronic signatures.

The submission by Amazon, in reply to the consultation on promoting Electronic Commerce, elaborated on concerns about the use of secondary legislation in a range of departments:

> Amazon.co.uk considers that the Government's proposed approach to empower Ministers to amend existing legislation to allow for electronic signatures and records is inadequate in that:
>
> - there is greater scope for inconsistencies to arise, given that the review is in the hands of several Ministers with possibly differing views on the desirability of such amendments;
>
> - the approach is dependent on individual Ministers giving priority to the review;
>
> - the fact that amendments are likely to be sporadic will create uncertainty for business and place an onerous burden on entities operating in the United Kingdom to monitor the state of the amendments and track which legislative requirements may be met electronically.[33]

On the other hand, this approach allows flexibility and a speedy response to issues arising from changes in the industry or technological developments. Any attempt to cover the topic in primary legislation would run the risk of laying down rules that might become obsolete or prove inappropriate. Restrictions of parliamentary time mean that the updating of primary legislation often has to wait for a free slot. Therefore delays might leave the industry with inappropriate legislation. Secondary legislation does offer flexibility, even if it also means that Ministers have greater freedom to act without parliamentary scrutiny.

---

[32] www.dti.gov.uk/cii/elec/billsumm.html (on the DTI website)

[33] *Amazon Co UK's submission in reply to the Government's consultation*, 8 October 1999

D. Part III of the Bill

This part amends the *Telecommunications Act 1984* so as to take account of the fact that there are now so many telecommunications operators licensed under the terms of this legislation. The Explanatory Notes show how the new sub-sections 12 (4A), (4B), (6A), (6B), (6C), (6D), (6E) and (6F) fit in to section 12 of the Act, as well as showing the context of the new section 12A. They also give further background.

Although this might appear to be merely routine tidying-up, there was a great deal of comment on it in the consultation exercise, which related to Part IV of the draft Bill, which appears to be identical to Part III of the current Bill:

> 28. Although nearly everyone who responded on Part IV recognised the problem which it addresses, most were unhappy about some aspects of the proposals. In general, the respondents wanted more certainty and a wider appeal mechanism.
>
> 29. The most common concern was over what might constitute a 'significant minority'. Some wanted the Secretary of State to be required (not just empowered) to make a 'rules and principles' order; others wanted the DGT's statement of his reasons for any finding that objectors do not amount to a significant minority, to be appealable. There were concerns that BT could be unduly favoured by these provisions, and calls for the criteria in 12A(9) to relate to the quality of the objections rather than, or in addition to, the number and size of the objectors. There was much favourable quotation of the EU Licensing Directive's requirement for regulatory procedures and decisions to be open, non-discriminatory, transparent, objective and proportionate.
>
> 30. Similarly, respondents wanted more consistent criteria, and consultation, on any finding that a proposed modification is 'deregulatory', with a wider right of appeal than just by the holder of the licence.
>
> 31. On appeals in general, there was a great deal of concern that the appeal processes envisaged by the Bill amount to little more than judicial review, whereas what is needed is a hearing on the merits, with a possibility for the appeal to go to the Competition Commission where appropriate. Other views on appeals were that the court should have power to award compensation etc; for deferral of any modification pending an appeal hearing; and for deletion of the word 'material' from 12B(2).
>
> 32. There was a view that the Bill's provisions are unsuitable for the particular situation in the mobile market, where operators have substantially different perspectives from each other. For example, it was suggested that in any market with six or fewer players an objection by any one of them should always be considered a significant minority.
>
> 33. Two respondents who opposed the Bill suggested, as an alternative way of meeting its objectives, simply that any operator's failure to respond to a modification notice should amount to a deemed consent.[34]

---

[34] www.dti.gov.uk/cii/elec/billsumm.html (on the DTI website)

IV European and International considerations

It is clear that it would be desirable to have the same law covering electronic transactions across the world, yet that is hard to achieve, partly because of the time taken to negotiate agreements, and partly because considerable differences of opinion remain about the appropriate way to act. Even in the British example, it is clear from the changes made to the draft Bill as a result of consultation that the decisions are far from simple. At an international level there would be bound to be disagreements. Many issues are not covered by new legislation and will presumably be covered by the existing legislation dealing with international mail order transactions by post or telephone. Problems will no doubt arise on a much larger scale as electronic commerce takes off worldwide – for example consumers not receiving the goods they expected or being overcharged on their credit cards – but there is no question of a completely new legal framework to deal with such issues at this stage. One issue remaining to be resolved is whether the law should specify which country's jurisdiction should be used when there are international disputes. Consumers tend to favour specifying the legal system of the purchaser, whereas suppliers favour specifying the legal system of the supplier, or leaving the question undecided.

There are two draft EC Directives, summarised here, relating to electronic commerce. Both of them are limited and do not prescribe detailed legislation. Indeed, they are rather like the original idea of Directives, which directed Member States to make legislation to achieve a certain end, whereas modern Directives often lay down detailed legislation in very much the same way as Regulations.

1 *Proposal for a European Parliament and council Directive on certain legal aspects of electronic commerce in the internal market*, EC Draft 5123/99 of January 1999

Executive Summary

> Electronic commerce offers the Community a unique opportunity for economic growth, to improve European industry's competitiveness and to stimulate investment in innovation and the creation of new jobs. But such benefits will not be optimised unless the many legal obstacles which remain to the on-line provision of services (particularly important for cross border trade and for SMEs) are eliminated. The present proposal intends to remove such obstacles thereby allowing our citizens and our industry to benefit in full from the development of electronic commerce in Europe.
>
> The Commission's 1997 Communication on electronic commerce set a clear objective of creating a European coherent legal framework by the year 2000. This proposal meets that objective. It builds upon and completes a number of other initiative that, together, will eliminate the remaining legal obstacles, while ensuring that general interest objectives are met, particularly the achievement of a high level of consumer protection. This proposal will reinforce the position of the Community in the international discussions on the legal aspects of electronic commerce which are currently underway in a number of international fora (WTO, WIPO, UNCITRAL, OECD). The Community will thus secure a major role in

international negotiations and significantly contribute to the establishment of a global policy for electronic commerce.

The proposal is based on the orientations set out by the Commission in the 1997 Communication. It provides a light, enabling and flexible approach. Particular attention has been paid both to the special nature of the internet and to the role of interested parties and of self-regulation. The proposal meets the principles of subsidiarity and proportionality by covering only those issues where a Community initiative is indispensable. These issues, which were also identified in the Commission's 1997 Communication, have been subsequently endorsed by the European Parliament. They are the subject of work at Member State and international level and are being discussed by industry and other interested parties.

At present, there is uncertainty in a number of areas about how existing legislation can be applied to the on-line provision of services. There is divergent national legislation already in place or currently being discussed. Furthermore, diverging jurisprudence is emerging. The proposal therefore seeks to remove the obstacles that result from such conditions, for service providers established in Europe, by tackling five key issues that together form a coherent framework to bring about the free circulation of on-line services. These issues are all inter-related because obstacles to electronic commerce services can arise at each step of the economic activity (from the promotion and the sale of a good or service to the settlement of disputes) and because none of these obstacles can be removed in isolation (for example, clarifying a service provider's liability is not possible without defining its place of establishment). Accordingly, the European Parliament, in its recent resolution, has asked the Commission to speed up the process of presenting a proposal for a directive which would address these issues in a coherent way.

These five issues are the following:

(1) Establishment of Information Society service providers

The proposal removes the current legal uncertainty surrounding this issue by providing a definition of the place of establishment in line with the principles established by the Treaty and the jurisprudence of the Court of Justice. This is a key element for the proper functioning of the Single Market. In addition, the proposal prohibits special authorisation schemes for Information Society services and sets out some information requirements that the provider must fulfil in order to ensure transparency of its activities.

(2) Commercial communications (advertising, direct marketing, etc.)

Commercial communications are an essential part of most electronic commerce services. It is therefore important to clarify and facilitate their use. The proposal thus defines what constitutes a commercial communication and makes it subject to certain transparency requirements to ensure consumer confidence and fair trading. In order to allow consumers to react more readily to harmful intrusion, the proposal requires that commercial communications by e-mail are clearly

identifiable. In addition, for regulated professions (such as lawyers or accountants), the proposal lays down the general principle that commercial communications are permitted provided they respect certain rules of professional ethics which should be reflected in codes of conduit to be drawn up by professional associations.

(3) On-line conclusion of contracts

Electronic commerce will not fully develop if concluding on-line contracts is hampered by certain form and other requirements which are not adapted to the on-line environment. To this end, Member States shall be obliged to adjust their national legislation. In addition, the proposal removes legal insecurity by clarifying in certain cases the moment of conclusion of the contract, whilst fully respecting contractual freedom.

(4) Liability, of intermediaries

To facilitate the flow of electronic commerce activities, there is a recognised need to clarify the responsibility of on-line service providers for transmitting and storing third party information (i.e. when service providers act as "intermediaries"). To eliminate the existing legal uncertainty and to bring coherence to the different approaches that are emerging at Member State level, the proposal establishes a "mere conduit" exemption and limits service provider's liability for other "intermediary" activities. A careful balance is sought between the different interests involved in order to stimulate co-operation between different parties thereby, reducing the risk of illegal activity on-line.

(5) Implementation

Rather than inventing new rules, the Commission has sought to ensure that existing EC and national legislation is effectively enforced. By strengthening enforcement mechanisms, the development of a genuine Internal Market - based on mutual confidence between Member States - is stimulated. Such strengthening is achieved by encouraging the development of codes of conduct at Community level, by stimulating administrative co-operation between Member States and by facilitating the setting up of effective cross-border alternative dispute resolution systems. For similar reasons the proposal also requires Member States to provide for fast, efficient legal redress appropriate to the on-line environment.

2 *Amended proposal for a Directive of the European Parliament and of the Council on a common framework for electronic signatures*, EC Draft 8264/99 of 12 May 1999

Summary

On 13 January 1999 the European Parliament adopted a legislative Resolution approving, subject to amendments contained in this resolution, the Commission proposal for a European Parliament and Council Directive on a common

framework for electronic signatures (COM (1998) 297 final - C4-0376/98 - 98/0191 (COD)) and calling on the Commission to alter its proposal accordingly.

The Directive aims at ensuring the proper functioning of the Internal Market in the field of electronic signatures by creating a harmonised and appropriate legal framework for the use of electronic signatures within the Community. It establishes a set of criteria, which form the basis for legal recognition of electronic signatures. The legal basis for the proposal is Art. 57 (2), 66 and 100A of the European Treaty.

The Directive establishes a legal framework for certain certification services made available to the public. It focuses particularly on certification services and sets up common requirements for Certification Service Providers (CSP) and certificates to ensure the cross-border recognition of signatures and certificates within the European Community. The Directive follows a technology neutral approach by covering a broad spectrum of 'electronic signatures'. It is based on a dual concept: CSP are in general free to offer their services without prior authorisation. In parallel, Member States are allowed to introduce, voluntary accreditation schemes based on common requirements and aimed at a higher level of security. The Directive is meant to contribute to a harmonised legal framework within the Community by ensuring that electronic signatures are legally recognised. To support the trust-building process for both consumers and business that rely on the certificates the proposal introduces liability rules for CSP. Co-operation mechanisms with third countries are embodied in the Directive to contribute to the global recognition of certificates.

Of the 32 amendments adopted by the European Parliament at First Reading, the Commission has accepted 22 in full (amendments 3, 11, 12, 14, 18, 20, 27, 30, 31, 32, 33 and 34) in part or in principle (amendments 2, 4, 5, 9, 13, 16, 17, 21, 22 and 25).

The Commission can not accept 10 of the proposed amendments for legal reasons (amendments 1, 10, 24, 28, 29), because, they contain superfluous provisions (amendments 6 and 7) or, because they would cause implementation problems (amendments 15, 23 and 26).

The Explanatory Notes to the new Bill state that it is consistent with the draft EU Electronic Signatures Directive, which is intended to harmonise the legal acceptance of certain electronic signatures throughout the EU. It states that it is also compatible with the OECD Cryptography Guidelines and the UN Commission on International Trade Law's Model Law on Electronic Commerce.

V The Second Reading Debate on 29 November 1999

The Minister (Ms Patricia Hewitt) stressed the aims of the bill:

> Our goal is clear. This country led the world into the first industrial revolution, and now we are determined to be winners in the new economy Our strategy for that is also clear. We need modern, competitive markets that will enable the fast growth of electronic commerce, confident consumers with the skills and access to exploit the potential of the internet; and a leading-edge Government, who are exploiting to the full the potential of the new technologies to transform the ways in which we deliver services to citizens and citizens communicate with the Government.[35]

She went on to explain the function of Part I of the Bill:

> The first aim of the Electronic Communications Bill is to build trust among consumers and businesses in the providers of trust services. There is widespread agreement as to the need for a kitemark, so that consumers and business alike can trust the providers of cryptography and confidentiality services. They need to be sure that messages will not be altered en route, that their credit card details will be kept secure and that their signature will not be misused. Our strong preference is for self-regulation, and I am working closely with the Alliance for Electronic Business, which is drawing up a self-regulatory approvals scheme. The alliance has made good progress; last Friday, I received an update, which I am urgently assessing. The proposals demonstrate the commitment of the industry to the self-regulatory approach--companies such as British Telecommunications plc, IBM and Royal Mail are involved.
>
> Our policy is underpinned by the principle of co-regulation, which is especially suited to the world of the internet. Co-regulation means that the Government should define the public policy objectives, but that industry should deliver the solutions through self-regulation.[36]

She pointed out that the criteria for judging a self-regulatory scheme had already been published, and said that Part I would be held in reserve, in case self-regulation failed. Then, in 2004, there would be an open review of how self-regulation was working, and, provided that it was working well, the powers in part I would lapse.

She then summarised the purpose of Part II:

> Part II deals with the conditions on which electronic transactions may take place between Government and the citizen…Part II also gives Ministers the powers to update the statute book by providing electronic equivalents to paper signatures,

---

35 HC Deb 29 November 1999 c 39
36 HC Deb 29 November 1999 c 43

> records and documents. Lawyers argue about whether electronic signatures would be recognised as valid by the courts, but we cannot afford to wait while lawyers argue and the courts decide. Instead, clause 7 will allow businesses and consumers to have confidence in electronic signatures, because it puts beyond doubt that a court can admit evidence of an electronic signature and a certificate in support of that signature not only to establish from whom the communication came, but to establish the date and time at which it was sent and whether it was intended to have legal effect.[37]

She said that it was anticipated that Clause 7 would come into force immediately the Bill received Royal Assent. The Minister then summarised Part III:

> Part III modernises the out-dated system for modifying telecommunications licences. There is widespread agreement in the industry that a more flexible and responsive approach to licence modification is essential. I have to say, however, that the industry was unhappy with our proposed mechanism, particularly the proposal that the Director-General of Oftel should be able to make modifications without a reference to the Competition Commission, despite objections, provided that those objections did not constitute a significant minority. Following our discussions with the industry, we have considered that proposal further and decided not to proceed with the "significant minority" concept.
>
> We are continuing to discuss possible alternatives with the industry. As I informed Opposition Front-Bench Members earlier this afternoon, I should like to make it clear that I will table amendments in Committee to simplify our proposals and ensure that they command wider support.[38]

Mr Alan Duncan, proposing an amendment to the motion, criticised Part I of the Bill:

> Part I is confusing and muddled. It is part statutory, part voluntary and, during the Minister's speech, the hon. Member for Broxtowe described the absurdity of companies not being compelled to participate, should its provisions be invoked. It is not needed at all. Indeed, the measure, which is part of a Bill for a fast-moving sector of the economy, is designed not to be used. It is designed as a dodo--it will lie on the statute book, extinct. She hopes that she will never have to invoke it, but, even today, has been unable to say under what criteria she might decide to invoke it.
>
> The whole point of part I is that it is bound to be overtaken by events and rendered obsolete by technological advance. At least there is a sunset clause, but I suggest that it would be better to invoke it now and not have part I at all. The Minister will perhaps have seen from her own mailbag--as I certainly have and

---

37 HC Deb 29 November 1999 cc 45-6
38 HC Deb 29 November 1999 c 47

> many other hon. Members will have today--that the Law Society recommends the total removal of part I.[39]

He was, however, content with Part II:

> The kernel of the Bill is part II--provision for electronic signature, which is all that the industry needs. It wants to know that there will be a proper legal framework within which a person can contract with another and that the contract will stand up in law. As the Minister rightly said, in many examples a handwritten signature is required - in many cases, it must be witnessed by someone else - but as the world advances it should be possible to achieve such verification and signature electronically. That is what the industry needs, and that is all that it needs, which is why we would have fully supported, even in the previous Session of Parliament, an e-commerce Bill that provided for electronic signature.[40]

He then dealt with Part III:

> Everyone recognises that part III is a bolt-on extra. Any provision that is retrospective, as the amendment of telecommunications licences would be, gives cause for concern. We reserve judgement on that. What matters is that existing licence holders are not disadvantaged. I am grateful to the Minister for explaining to the House that she will consult more widely and that she intends to remove some parts of the Bill in Committee. We are getting nearer to the four-page Bill that we would like.[41]

He added some more general criticisms of the powers granted to Ministers to make regulations.

Mr Baldry spoke on behalf of the Trade and Industry Select Committee:

> It would be fair to say that the Select Committee welcomed the Bill. We welcome clause 13, which is in part III. It is a crucial new provision that responds to the Select Committee's recommendation that the Bill should explicitly exclude the use of key escrow as a criterion for accreditation under a statutory regime. Of course, more information is required on some subjects. In particular, information is required on the timetable for the commencement of parts I and II, on a draft of theT scheme and on its start date, which will be independent of the Act, and on the level of fees. Doubtless, such issues will be dealt with in Committee.

---

39 HC Deb 29 November 1999 c 54
40 HC Deb 29 November 1999 c 55
41 HC Deb 29 November 1999 c 56

> Some measures have been added to the draft Bill that require explicit justification. They include the clause 8(3) change to relax the criteria for record keeping of electronic storage or communication, and the clause 9(6) rider, which expands the scope of orders made under clause 8. Part III, which was formerly part IV, on telecommunications licence modifications, is not only an ever more evident add-on, but raises fresh unease because it will give added powers to the director to decide what constitutes a significant minority for objections. There has been no sign of movement on the process for changes deemed regulatory, but it is balanced by an attempt to clarify grounds for appeal.
>
> I suspect that the members of the Select Committee and of the Standing Committee will want to ask specific questions. It would unfair to detain the House on those points now, because they are matters for Committee. However, it will be good if the Government can keep the House and industry abreast of the implementation dates for various provisions in the Bill. They are not always self-evident from the Bill and people will want to know when the different provisions will apply.
>
> Although it is a narrow Bill, its provisions are clearly worth implementing. I hope that the kitemark of approval and the Bill itself will start to encourage consumer confidence. The hon. Member for Stevenage (Barbara Follett) made a sensible and proportionate contribution and she made it clear - I think that everyone would agree with this - that although the internet and e-commerce are expanding exponentially, huge numbers of people are wary of using the internet simply because they are worried about fraud. If the Bill can help reassure consumers that such fraud will not take place, it will promote consumer confidence and e-commerce in this country. Whatever we do in legislation, concerns will remain with which legislation simply cannot deal. In an earlier report, the Select Committee expressed concern about what is known in shorthand as the "digital divide", through which the poor and the elderly feel excluded from the internet. It is not easy to legislate for that problem, but public policy should be concerned about it. As public policy makes provision for services, such as NHS services, to become more readily and more easily available on the internet, we must recognise that, for all sort of reasons, some people will for a long time find the internet difficult to use.[42]

Points raised by other speakers included; concern about the high charges for internet access and use in the UK (c 70); proposed fees for certification in Part I (c 87); and concern whether self-regulation would be sufficient (c 91).

---

[42] HC Deb 29 November 1999 cc 79-80