INTERNET COMMERCE:
THREATS AND OPPORTUNITIES

- *Background to DTI's latest proposals on security*
- *Electronic business and erosion of the tax base*
- *Content regulation*

Although slow to start, electronic commerce over the Internet is growing fast and making it necessary to address key issues which will determine the way in which this truly global marketplace develops.

This note explains some of the arcane and complex related issues (e.g. encryption).

E- COMMERCE AND THE INTERNET

The Internet has long been in the news as a means of spreading information, as a way of communicating and increasingly as a means of advertising. Many companies have also turned to the Internet to add an extra dimension to their existing business, and there are also companies which have set up from scratch and operate exclusively in an Internet environment. This is pushing to the forefront technical issues such as encryption, how Internet business should (or could) be regulated and managed, and also how such 'e-business' ties in with the tax system. These issues are not trivial - the UK is the fourth largest IT, electronics and communications (ITEC) consumer worldwide and has the fifth largest ITEC industry (£43B or 6.7% of GDP). This is a strong base from which to develop e-commerce which is expected to become a significant fraction of global GDP (see **Box 1**), making 'globalisation' and 'virtualisation' significant terms for the UK and other nations.

ENCRYPTION

Electronic commerce has always used encryption. Thus when banks or financial service companies transfer electronic funds, or an ATM communicates to validate a customer's PIN number, messages are encrypted to guard against interception and fraud. These procedures are not, however, suitable for providing security over open networks such as the Internet since:

- Traditional models of e-commerce involve only a few participants, and those sending and receiving messages can use the same encryption software and secret key. In contrast, the Internet allows business with new customers from anywhere in the world, and it is impossible for everyone to have a 'secret key'. A very different approach is required.
- Because customers and vendors may have no prior knowledge of each other in Internet commerce, electronic means are needed to verify identities - so that a customer sending money to a company's web page knows it is not fraudulent; so that one party cannot deny or renege on a commitment, and so a third party cannot easily interfere and change a message (e.g. the terms of contract).

POST **114**
TECHNICAL REPORT
April 1998

POSTreports are intended to give Members an overview of issues arising from science and technology. Members can obtain further details from the PARLIAMENTARY OFFICE OF SCIENCE AND TECHNOLOGY (extension 2840).

BOX 1 COMMERCIAL USE OF THE INTERNET

Electronic commerce has been growing for many years, and links companies to suppliers, financial institutions together, and business to Government. While business over the Internet is small in comparison, it will become increasingly important because of:

- Mass access - there are already approaching 100M people connected via their computers to the Internet, and new interactive digital TV is likely to offer much easier access to the World Wide Web (WWW).
- There is a general trend toward harmonising current standards (such as CALS, EDI, etc) with Internet standards for all data networks, which will make it easier for business to use the Internet for business to business contact.

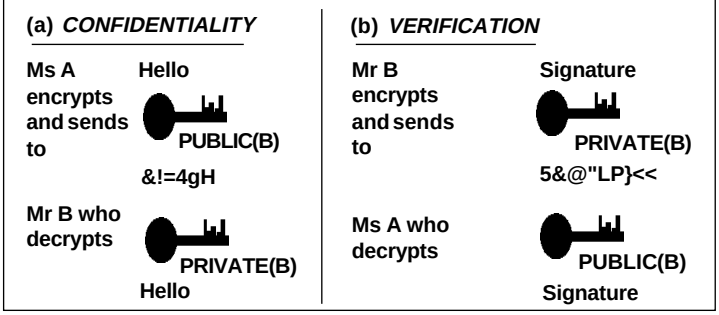
The number of commercial web sites passed 250,000 in 1996 and is still rising fast. The 'old' e-commerce required specific relationships between organisations and individuals. The wide-open market via the Internet, however, means that anyone with a computer and Internet access can become a merchant and reach customers all over the world; the consumer equally can find out about and buy products offered anywhere. This throws up very different challenges, opportunities and risks. It can offer companies:-

- a new advertising channel;
- a new means of reaching customers and receiving orders;
- cutting out the middle-man by direct sale - airline tickets, books, wine, etc. (called 'disintermediation');
- establishing new 'virtual' enterprises, or 'virtualising' existing ones;
- developing and selling new digital products (e.g. software, WWW support services);
- replacing physical goods (e.g. games, books, music) with their digital equivalent.

Estimates of the growth of e-commerce as a whole are rather speculative still and often fail to differentiate between business over secure intranets and over the public internet. Nevertheless, the business conducted over the Internet is expected to rise dramatically - to equal that from mail order sales by year 2000. For example, direct airline ticket sales may reach $5B per year by 2000; one online bookshop sold 6.5 million books in 1997 alone (although this and other operations have yet to be profitable). Some industry estimates are however much higher - e.g. IBM anticipate Internet commerce reaching $200 billion by 2000.

As described in **Box 2**, one solution to these challenges is public (or dual) key encryption, which works as follows. The company that wishes to do business over the 'net' obtains a set of **public and private keys** and sets up the appropriate software on its computer systems. It then makes its **public key** available to anyone who wishes to communicate with it. When a customer sends a message, he / she uses the computer to encrypt

FIGURE 1 PUBLIC KEY ENCRYTPION



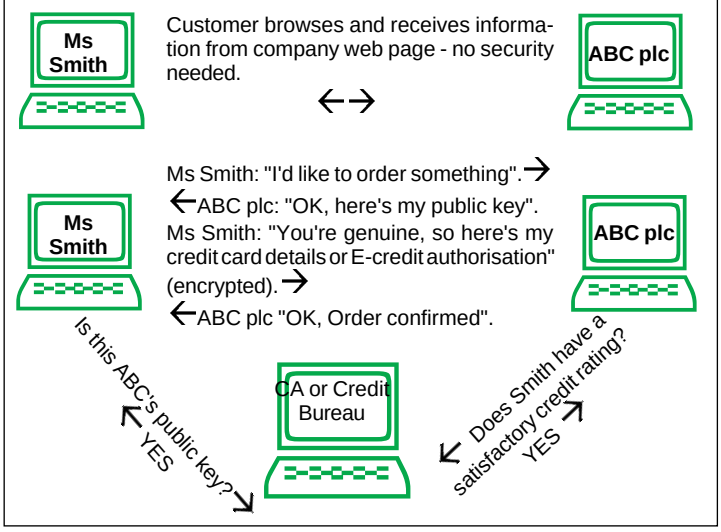
with the public key, after which it can only be de-crypted by the company's **private key.** The 'magical' feature of the mathematics involved is that even the sender cannot de-crypt the message once it has been encrypted using the public key (**Figure 1**).

Another property of the mathematics involved is that if the reverse takes place - i.e. a message is sent by the company with its private key, this can be de-crypted by any holder of the public key. If, however, it has been tampered with in any way, this will no longer work, and thus the ability to de-crypt is proof that the message is genuine and has not been tampered with. The same techniques **thus allow either party to electronically sign the document**.

To allow companies to do business with any potential customer, the public keys have to be available - just as the telephone and fax numbers are in business directories. Making the public keys available in this way has several implications. Such information needs to be relatively centralised, so people know where to go for it; there needs to be some method of ensuring that the keys published do actually belong to the company or individual concerned, and that the transaction is reliable. A number of bodies offering such services (**Certification Authorities** -CA) have already been set up. For instance, US companies such as 'Verisign' and 'Cyberscript' allow a customer's computer to check the identity of the company and the validity of its public key (see **Figure 2**). Other organisations are developing similar services - e.g. Natwest and Barclays Bank have agreed a legally-binding system for 'digitally signing' on-line forms submitted to the UK government. The market is thus responding to the need for security and authentication without government intervention.

The strength of public key encryption described in **Box 2** is related to the length of each key and beyond a certain limit (perhaps 56-bits or longer), the encrypted message becomes 'uncrackable' even with the most powerful computers. **Advances in encryption techniques are thus a two-edged sword** - strong encryption makes legitimate commerce very secure; it can also help human rights groups investigate without their reports being decoded by those whose record is being investigated. But at the same time, strong encryption

FIGURE 2 SECURE INTERNET TRANSACTIONS



could be used by organised crime to make its communications and money transfers essentially uncrackable by law enforcement agencies; equally, national intelligence agencies' ability to intercept and decode foreign intelligence material could be compromised. **It is how to strike a balance between these 'costs and benefits' of strong encryption that gives rise to the current policy debate**.

The more powerful encryption techniques have been subject to export controls for some time on the grounds of national security. As described in Box 2, there have been several attempts in the USA at striking a 'deal' which maintains preferential access by intelligence and law enforcement interests to encrypted messages, as the 'price' for allowing export of the technology. The current policy debate centres on what methods should be used to recover keys in order to decrypt messages. One route is to require users of strong encryption to deposit a copy of their private key with an independent '**Trusted Third Party**' who would be required to give it up to appropriate judicial or ministerial authority (**key escrow**). Another is where the encryption software involves registration with a **key recovery agent**.

The last Government's proposals in this field were set out in a consultation paper released in March 1997 - this proposed a licensing system for "Trusted Third Parties for the Provision of Encryption Services". Under these proposals, there would be no interference *per se* in the private use of encryption, but anyone offering encryption services to the public would have to be licensed by the DTI, and a condition of licensing should be that private encryption keys should be deposited at the TTP, and should be provided within one hour of receipt of an executive or court order. Since the market for unlicensed TTPs could be limited, these proposals were seen by many as equivalent to mandatory key escrow, and raised objections.

BOX 2 DUAL-KEY ENCRYPTION AND KEY ESCROW

Before 1976, both ends of an encoded message needed the decryption key which had to be sent separately, effectively restricting cryptography to parties who already had a trustful relationship. Breaking out of this 'strait-jacket' completely revolutionised cryptography and followed from some rather counter-intuitive properties of large prime numbers.

Basically, if one takes 2 large prime numbers, one can work out 2 other numbers which can serve as a set of private and public encryption keys. With the **Mr B's public** key, Ms A can send a confidential message to him which he can decode with his private key. However, the mathematics involved is 'one-way', and the public key cannot decrypt the message it has encrypted - thus the message to B is secure. There is, of course, a mathematical relationship between the public and private keys, but it is complex and provided the numbers are big enough, can exceed the ability of even the most powerful computers to 'crack'. Thus a completely secure communication can occur between two parties without prior negotiation of a shared secret key.

This breakthrough (RSA, asymmetric or public key encryption) remained largely unused commercially because it was protected by patent, and its use outside the USA restricted by US export controls (for security reasons). However, in 1992, RSA was adapted for PC-users by a US computer security consultant who made this public as PGP ('Pretty Good Privacy'). Despite official USA efforts to suppress PGP, it is now widely available via the Internet.

Official US bodies were concerned at the possible spread of such 'strong' encryption technology because it could make it impossible to intercept and decode communications in criminal and national security situations. It proposed in 1993 to keep control through a device known as the 'Clipper' chip - a tamper-proof chip manufactured under Government licence which would contain the encryption program itself. Individuals would have the chip (and associated cipher key) to use as they wished, but a copy of the private key would be lodged with a US Government 'escrow' agency, which would release it under specified conditions (e.g. in response to a court order). Anything generated by that chip could then be deciphered.

This proposal was opposed widely by US civil liberties groups and seen by interests outside the USA as offering a 'trapdoor' for US authorities to commercial traffic. Serious technical shortcomings led to new policies where private keys would be held by 'Trusted Third Parties' who, would have the responsibility of responding to court warrants, etc. US companies could also export encryption of key lengths of 56 bits or less (a length which may be 'crackable' anyway), providing the industry worked to develop 'key recovery products'. These now exist and mean that when a company uses one these products, it has to register with a key recovery agency. This is not the same as depositing the private key, but still allows targeted traffic to be deciphered via a knowledge of the key recovery agency and the customer's public keys.

CURRENT ISSUES ON TTPs

The basic market needs for a CA / TTP include:

- maintaining unique identifiers for individuals and organisations, and generating key pairs;
- certification (validation of each names' public key);
- key management -for keys used for validation and signature; and for maintaining confidentiality;
- storage of encrypted data, key recovery services;
- security services for validation, time-stamping, non-repudiation, etc.
- agreement and enforcement of contracts between parties who only meet in 'cyberspace'.

At present, such services are provided by the market at low cost and are integrated 'unseen' into browser and other software (Figure 2); meanwhile new CAs / TTPs can be set up to serve particular markets - for example the banking sector might wish to establish its own 'internal' TTP system, while other bodies such as the Post Office, solicitors, or quality control bodies could offer more widely available services. Development of such services is however seen as needing **regulatory certainty over what conditions of licensing will be applied**. The 1997 proposals received much support on the principle of establishing a licensing scheme, and also because they sought to encourage alternatives to the current situation where advanced encryption software often involves relying on US key recovery agents which are responsive first to US law enforcement agencies. They were however criticised on the grounds that:

- adding key escrow to the role of the CA created a potential risk to the customer's security, as well as an organisational burden which could limit the number of bodies able to offer such services and add to costs;
- ways of evading 'legitimate' encryption exist - keys need not be escrowed or other encryption techniques used (e.g. steganography 'hides' messages in digital data of a picture or music score). The proposals could thus have brought cost and complexity to law-abiding users while not achieving the results desired by law enforcement agencies;
- the global nature of such schemes introduce jurisdictional issues of extra-territoriality[1];
- depositories of many secret keys could be an irresistible target for hackers or criminal / terrorist interests.

Such questions are not unique to the UK and encryption has to be recognised as an international issue in which many players are currently operating. In the USA, current legislative proposals link licensing of TTPs to key escrow, but licensing would remain voluntary. The OECD agreed a number of principles in March 1997 which, while recognising that key escrow could be required in certain circumstances, also warned against *"unjustified obstacles to international trade and the development of information and communications networks (8th*

1. One single TTP world-wide is clearly impractical, so there would have to be one or more networks of TTPs to bridge national and international legal frameworks. Thus a British TTP would have to comply with UK law, but would have to be trusted internationally in order to fulfil its role; equally, there would have to be restrictions on bodies offering services outside the UK to evade UK licensing conditions.

principle)" and *"legislation which limits user choice (2nd principle)."* The 5th principle states that: *"The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods"*.

Independent experts saw the former Government's proposals as going beyond the OECD position and essentially leading to mandatory key escrow and an expansion in the capabilities of surveillance authorities to access and decode routine traffic. As such they attracted opposition from industry which saw them threatening vulnerability to fraud and industrial espionage, while also being linked to one technical approach to encryption at a time when technology was bringing in a range of alternative encryption systems to maintain confidentiality. The value of private key encryption is now increasingly for verification - exactly the area where key escrow is undesirable.

Many anticipate that the DTI's revised proposals (expected imminently) will reflect these concerns and provide for a more voluntary regime with less demanding conditions for private key escrow. It will also recognise the importance of attaching conditions only to confidentiality keys (and not those for authenticity, where national policy will need to mesh with a proposed EU draft directive on digital signatures). Independently of any regulations, the UK industry (via the Alliance for Electronic Business) proposes a voluntary 'Trust Services Infrastructure' whereby CA / TTPs would be able to join a UK Trust Services Association acting as a 'voluntary' regulator to ensure appropriate standards of competence and trustworthiness of member bodies. It would also work to develop a 'Global Trust Infrastructure' through coordination and mutual recognition of equivalent bodies overseas.

Even with DTI's new proposals, tensions will still remain between the interests of efficient e-business (flexible strong and cost-effective encryption services) and those of law enforcement and intelligence agencies which still need access to suspicious communications. Those in the industry see the primary goal as an unrestricted market for strong encryption products which is globally interoperable, but wish to work with Governments (US and EU) to define conditions of access for law enforcement purposes etc. without mandatory key escrow.

The ultimate solution to this quandary is not yet defined, but many point out that the 'genie' is already out of the 'bottle' and strong encryption which does not depend on public key encryption is in use making reliance on key escrow too technology-dependent. At the same time, those concerned to thwart interception can use their own keys or other techniques to evade controls. Many thus argue that it is important that the legitimate needs of interception, surveillance and decryption take full account of these realities and ensure that the necessary measures are both technology-independent and avoid stifling legitimate commerce or rendering it vulnerable to industrial espionage. One option cited by some would be to strengthen the law to make it an offence to refuse to decrypt specific transmissions or data targeted by a judicial warrant (or to require them to provide hard copy of the original transmission). A parallel approach may need to recognise that the volume of e-traffic is now so large and growing so fast[2] that much greater selectivity is needed to identify those transmissions of interest, and to recognise a greater role for sectors of business to regulate themselves - perhaps under more official guidance (e.g. via codes of practice) on security, access control, and how to identify and respond to suspicious traffic.

INTERNET COMMERCE AND TAX

Governments are clearly interested in the potential macroeconomic effects of Internet commerce. Some of these will benefit consumers who will be able to shop globally for the best prices on goods and services, potentially levelling heretofore distorted markets (without the need for complex intergovernmental trade negotiations). On the deficit side, Internet commerce may diminish the ability of government to raise taxes on goods, services or income.

The current complex web of national and international tax legislation has evolved around conventional models of business - where physical goods are bought and sold, and where customers and suppliers have a place of residence. As increasing amounts of trade have involved less tangible items such as financial and telecommunications services, tax agreements have adapted accordingly, but the potential growth in Internet-mediated business could pose real challenges to the ability of Government to maintain revenues. These issues are being addressed in a number of fora, for example by the OECD's Committee on Fiscal Affairs, and also within the EU. This subject is complex and still very fluid, and thus only key questions are outlined in **Box 3**, relating to the twin problems of how best to avoid tax evasion or double taxation.

Overall, internet commerce impacts most severely on the two key concepts of **residence** and **source**. For instance, is a computer server connected to the Internet in a country in which the enterprise has no other presence, a 'permanent business establishment'? Or should tax status be related more to the support, storage and distribution centres? Even where it is possible to establish where the enterprise is located for tax purposes, the ability of residents to establish off-shore

2. In 1997, the number of e-mails (2.7 trillion) was five times the number of paper mail delivered worldwide.

BOX 3 INTERNET COMMERCE AND TAX SYSTEMS

Internet commerce brings in several areas of complexity with which existing systems have never had to deal. Some of these are:-

- The 'entry costs' to global markets have been reduced and made it accessible to many small companies, leading to rapid expansions in cross-border activities.
- Many constraints on physical location are removed. The 'front office' may be 'virtual' and no more than a computer system with communication links, and infinitely mobile. Internet business can involve many countries (one for the 'web' site, another for product storage and distribution; other national networks carry messages). It is thus difficult to define where an activity is carried out.
- It can be difficult to identify participants in Internet commerce - for instance the web page address provides no information on where the machine is located.
- The removal of intermediate institutions removes the main tool for revenue collection - intermediate taxing points.
- E-commerce may increasingly involve new forms of electronic money not readily recognised by the tax system.
- E-commerce may replace physical goods (e.g. CDs) which can be taxed crossing borders. The digital equivalent flows unnoticed across communications links.
- Tax havens and off-shore banking facilities become more accessible, allowing more people to use these to reduce or avoid taxation. Internet banking offers high degrees of anonymity and immediacy of funds transfer.
- With detection and enforcement, E-commerce provides far less evidence of transactions than traditional commerce. Disintermediation may also mean that the contracting parties are unaware of withholding obligations. Encryption will also contribute to the near impossibility of tracking all movements and conducting audit trails.

A parallel set of issues affects the collection of consumption taxes, such as VAT.

- Place of supply is a critical concept in VAT which presumes a fixed establishment. Internet transactions could need to be treated in the same way as telecommunications services, and taxed at the customers' end.
- The difference between goods and services is blurred by Internet commerce. This is particularly important where it relates to goods imported from outside the EU, where currently they are liable to VAT at importation. Downloading the physical good as data may allow VAT to be avoided altogether.
- VAT rules distinguish between different services, which become difficult to differentiate when all data are digitised.
- Even with off-line services involving the transfer of goods across borders, the increased volume of international traffic may well swamp the ability of customs authorities to collect tax.

companies could lead to a tax-driven migration of businesses to the Internet and Internet businesses to low tax jurisdictions. Combined with the anonymity and potential for evasion, this could have major implications for tax recovery. By making source income increasingly difficult to track, the growth of new electronic commerce may lead to the criterion of residence-based taxation assuming greater importance. The increasing globalisation of companies may also increase their flexibility to set transfer prices between different parts of the business to minimise overall tax liability. Such issues can be slow and difficult to resolve - as illustrated by the persistence of the Service Provider anomaly where EU-based SPs charge VAT but those based outside the EU do not.

The difficulties foreseen in maintaining tax revenues have led some to call for alternative, more direct taxes on Internet activity - for instance a 'bit tax', which would apply to the volume of data, irrespective of its underlying value. Many UK Internet users already ay the equivalent of such a tax, in that they pay VAT on their telephone call to connect to a service provider, but the bit tax would be specifically linked to the amount of data traffic. Such a tax could, however, present many problems -for instance, it could not discriminate between high volume / low value uses (e.g. telemedicine) and low volume / high value transactions (e.g. selling shares). It could also be an unstable arrangement - as the volume of data on the Internet increases, presumably the tax rate would have to be constantly adjusted. The question of bit taxes is thus not being seriously examined in the various international groups involved, indeed it would go against one of the areas of agreement between the EU and USA on Internet Commerce - that taxes should not be heavier on the Internet than on traditional commerce (see later). Moreover, the USA has proposed that, at least in the initial stages, the Internet should be declared a tariff-free environment, whenever it is used to deliver products or services (this does not exclude it from tax liabilities when it is used in the same way as a mail order service).

Such considerations have led to extensive debate and consultations. For instance, the US Department of the Treasury has put out a very detailed analysis of the implications above, as part of an overall consultation; the OECD Committee on Fiscal Affairs has organised various discussion documents and meetings to try and identify consensus on the way forward. The UK Treasury, Inland Revenue and Customs and Excise are engaged in these international activities.

OTHER REGULATORY ISSUES

The USA sees the Internet as having a potentially profound effect on the global trade in services, whether these involve computer software, entertainment products, information services, product licences, financial and professional services, or in terms of direct retail sales and marketing where customers are able to shop in their homes for products from all over the world.

The above applications potentially raise problems which could lead to governments attempting to regulate. For instance, different national regulations for professional qualifications make trans-border profes-

sional services potentially problematic. The laws a consumer relies on for protection at home might not apply in the country selling the service, and thus redress (e.g. refunds) might be difficult to obtain. 'Contracts' agreed in Cyberspace might not fulfil national legal requirements. Supporters of Internet commerce see considerable dangers if national governments (or the EU) react by imposing extensive regulations on the Internet and electronic commerce, arguing that this would stifle it before it has attained economic viability. Potential areas of regulation foreseen included taxes and duties, restrictions on the type of information transmitted, control over standards development, licensing requirements and rate regulation of service providers, measures to 'protect' the consumer, and other potential regulations (e.g. on digital signatures).

In an attempt to avoid such a scenario, the USA proposed a "Framework for Global Electronic Commerce", which should follow the primary principles espoused in **Box 4**. These are essentially the same as the UK Government's own four principles:

- The law should apply on-line as it does off-line, with the result that each person is responsible for their own conscious acts and omissions.
- Need international co-operation between enforcement authorities in different jurisdictions, and between legislatures where harmonization of existing laws is possible (e.g. a Uniform Commercial Code).
- Businesses and consumers should have access to tools enabling them to protect themselves (e.g. rating/filtering for harmful content; digital signatures for verification etc.).
- Service providers should take voluntary action to uphold the law on-line, while government keeps an open mind on possible needs for future regulation.

The EU has also accepted the need to avoid 'regulation for regulation's sake', but has identified a number of areas where electronic commerce poses challenges, which, in the Commission's view, require action under the Single Market framework (see also Box 4). Some of the early proposals under these headings are already raising concerns in industry about their potentially inhibitory effect on the growth of e-commerce within the Community. For instance, Commission proposals on digital signatures need to avoid being technology-dependent (e.g. recognising only the use of public key encryption), thereby excluding other approaches which might be acceptable to the market. Some ideas on 'consumer protection' have also suggested introducing a requirement that terms and conditions be provided in hard copy, before an electronic transaction can be confirmed, which would rather go against the purpose of e-commerce to eliminate such steps! Supporters of e-commerce point out that there is much potential for self-regulation which has already evolved without the intervention of regulators. For example, unsatisfactory products can attract a refund from credit card operators and offending merchants could be taken off card companies' lists of approved vendors.

BOX 4 US AND EU POLICIES ON INTERNET COMMERCE

The US "Framework for Global Electronic Commerce" (The White House, July 1997) set out 5 principles for policy on e-commerce:

1. The private sector should lead, with governments encouraging industry self-regulation.
2. Governments should refrain from imposing new and unnecessary regulations, bureaucratic procedures or taxes and tariffs on commercial activities over the Internet.
3. Where government intervention is necessary, its goal should be "minimalist" - to ensure competition, protect intellectual property and privacy, prevent fraud, foster transparency, support commercial transactions and facilitate dispute resolution.
4. Existing laws that may hinder electronic commerce should be reviewed or eliminated.
5. The legal framework supporting commercial transactions on the Internet should be governed by consistent principles across state, national and international borders.

The EU/US Summit in Geneva (5 December 1997) reiterated the principle of market forces, but also committed (*inter alia*) both sides to work towards:

- A global understanding that when goods are ordered electronically and delivered physically, there will be no additional import duties applied in relation to the use of electronic means. In all other cases of electronic commerce, the absence of duties on imports should remain.
- Ensuring the effective protection of privacy with regard to the processing of personal data on global information networks.
- The creation of a global market-based system of allocation and governance of Internet domain names which fully reflects the geographically and functionally diverse nature of the Internet.
- Active support for the development of self-regulatory codes of conduct and technologies to gain consumer confidence in electronic commerce (including involving all market players and consumer interests).
- Close co-operation and mutual assistance to ensure effective tax administration and to combat and prevent illegal activities on the Internet.

Some specific EU Measures are starting to emerge. For instance, a draft directive has just been released on Digital Signatures, the Regulatory Transparency Directive may affect e-commerce in its extension to services. The EC is also establishing principles for content regulation by service providers.

Some need for regulations is foreseen however -e.g. to define the requirements for electronic contracts to be as valid as paper ones. But when needed, there is a wide consensus that they need to be international or internationally coordinated, and technology-neutral, in view of the rapid changes involved. An example of such a light regulatory touch might be to establish the framework for legal recognition of digital signatures, but enabling any technology to be accepted as producing a digital signature providing it meets general requirements of reliability, unambiguity, etc.

With the dominance of the USA in the Internet's history and current usage (80% of Internet traffic is in the USA),

BOX 5 RESTRICTING UNSUITABLE CONTENT

Censoring or jamming undesirable or illegal content faces two primary challenges - first, deciding on what is to be restricted, and then actually restricting it.

Most material on the Internet is generally available in other formats by other means. What the Internet does is allow individuals or small groups a huge audience at little cost. Some of these society may well regard as 'deviant' and object to, but there are many more groups (e.g. for disabilities) which use the Internet to their benefit, and there is widespread resistance to interfering with the 'freedom' of the 'Net' among its users.

The Internet is not, however, a law-free zone - material that is illegal off-line is also illegal on-line, and criminal liability falls on those who hold and access clearly illegal material, such as child pornography. The global nature of the Internet may, however, make such principles difficult to enforce. Outside cases of clear illegality, defining what is undesirable faces the same problem as for material available by other means. For example in the UK, defining what, under the terms of the Obscene Publications Act (1989), would 'deprave and corrupt'.

Where materials are held to be illegal, how can one go about removing them, given the difficulty of assigning responsibilities in the complex web of the net. After all, the **content provided** may not originate in the UK, or be put on the net in an area where the material is not illegal. Since UK law does not extend outside the UK, most attention has focused on the Service Provider's (SP) responsibilities in controlling content since these companies provide the Internet connection, and access in the UK itself.

Technical filtering of the broad contents of all sites is theoretically feasible, but the computers need to be primed with key words to search for, or some other guidance. Much filtering software has the problem of blocking out perfectly legitimate sites along with those dealing in, for example, sexually explicit images. Such systems cannot, therefore, even in principle be relied on to make statutory judgements, although they can raise alerts about material with particular characteristics - for instance, racist words, explicit sexual language, flesh tone in a graphics file, violence, and alert individual users to exercise their own choice.

The most promising approach is **voluntary content labelling**, possibly backed up by access providers making it a condition that all material posted is so labelled. Once labelled, it is a simple job (either for the SP or user) to apply a filter and to restrict use to specified ratings. Such an approval system is under development by the **Platform for Internet Content Selection (PICS)**. Other methods of making it more difficult to post undesirable material include a requirement for subscribers posting content to explicitly identify themselves, and providing SPs the ability to monitor and sample content to ensure the accuracy of conten labels.

While such technologies would make it easier to filter out undesirable content, they still place much of the responsibility on the individual user to ensure that their wishes are being met. Broad efforts to 'clean-up' the net are almost bound to be doomed to failure, even after the adoption of a rating system because the technical complexity of the system and the sophistication and motivation of many of its users will always leave loopholes.

there are concerns at the potential use of the international regulatory regimes to advance national economic interests. Thus the USA already exports $40B per year of goods and services in the categories for which Internet commerce is seen as a medium of growth, and thus maintaining the Internet as a 'free trade' zone can be seen as very much in the USA's economic interest. Some see the EU countries' failure so far to develop a common position on issues such as encryption that is also acceptable to the Middle Eastern and ASEAN nations, as assisting the USA to impose its own trading and regulatory regimes, as well as making it difficult for European suppliers to develop a viable market for their encryption products. Notwithstanding these concerns, progress is being made towards a common viewpoint between the USA and the EU, and a joint statement following the EU/USA summit in Geneva (December 1997) reiterates the principle of market forces applying in the Internet, and commits both sides to working towards the objectives in Box 4.

One area which illustrates the limited power of regulatory authorities when faced with the global phenomenon of the Internet is what to do about public concerns over **illegal and harmful content**. As explained in **Box 5**, the technical challenges of an effective means of filtering out undesirable content are complicated by the Internet's global reach, the variability of 'illegal or harmful' content between different countries, debate over responsibilities of content providers, service providers etc., and the fact that with thousands of web sites setting up each day, and thousands closing, comprehensive content scanning would be almost impossible.

As described in Box 5, the main approach being pursued in the UK is voluntary self-regulation - whereby as soon as a SP is aware of illegal material it is under an obligation to remove it (or face legal liability as an accessory). At present, sites are identified primarily through a 'hot-line' run by the Internet Watch Foundation (IWF) - an industry-funded group which receives, vets and where necessary acts on reports. Where content is deemed illegal, the sites are removed from the SP's servers and where appropriate, police advised in the UK or other countries. Although child pornography has been the primary focus so far as clearly illegal, other categories exist which may also be illegal - e.g. disseminating bomb-making recipes, advice on how to make fraudulent bank notes. But the main volume of traffic comes in the greyer area where it may not be illegal but is offensive to many, such as adult pornography, racist material or personal slander.

Here the emphasis is very much on making it easier for individuals to restrict their (or others such as children) access according to ratings on sex, nudity, language and violence. Some web sites already carry such a rating (e.g. from the Recreational Software Advisory Council - RSAC), and modern Internet browsers can be instructed to 'screen out' sites with particular ratings (or those without any rating). The IWF and analogous

bodies in other countries see this as the way forward rather than national regulatory authorities attempting to control content further. Indeed, the USA explicitly supports the broadest possible free flow of information across international borders, rejects the types of content regulation applied to radio and TV, and sees dangers that attempts by nation states to regulate content could disguise trade barriers as attempts to maintain cultural or ethical values. The current regulatory inconsistencies whereby the Internet offers access to material which would be banned (or subject to prosecution) if delivered by conventional broadcast media will thus continue and users will remain very much 'on their own' when it comes to protecting their interests.

There are many other issues relating to the 'Information Society' which have been covered elsewhere[3] - intellectual property protection, data privacy etc. However, one important management issue is the apparently mundane question of how people or organisations are awarded their 'domain' names- the electronic 'addresses' of the Internet web sites. Thus the UK Parliament's web address is **www.parliament.uk**; that of the White House is **www.whitehouse.gov**; such domain names have clear advantages over their electronic equivalent (a string of eleven numbers). As the Internet has expanded however, the difficulties of a company obtaining the domain name it prefers have grown, and new ways of allocating these are being sought. As the Internet essentially grew out of a US research network, the US National Science Foundation set the original name allocation system up, but the US Government is seeking to privatise these functions, introduce competition and make them more accountable to the user community.

There are many different communities that use the Internet - individuals, academics, business and, increasingly, governments, etc. and finding a consensus on this is proving difficult. Domain names can have a high commercial value, and there are an increasing number of disputes over registered 'trade names' etc. The proposed replacement for the current system with US private registrars has caused concern, particularly outside the USA, and the Internet's Policy Oversight Committee, has put forward proposals to increase the number of names available, and to diversify their management into a more international framework. This issue is not yet resolved, but again emphasises the importance of developing a timely EU-wide view so that foreign users of the Internet are not disadvantaged - perhaps through 'the Bangemann proposals' for a new international framework for Internet management, along the lines of other international bodies such as OECD and WIPO.

Other issues arise from the '**convergence**' between telecoms, broadcasting, and computing in the Internet and also the many different services (financial, retail, marketing, etc.) delivered over it, which can involve several different regulators. The DTI will be consulting later in the year on the implications for the regulatory system of digital convergence, and there have also been calls (e.g. via the EC's 1997 Green Paper) to re-examine the role of the many regulators involved, to eliminate inappropriate cross-over in their responsibilities and provide a simple system of protection for consumers, businesses and the public interest. In this context, the DG of OFTEL recently called for existing bodies to be rationalised into two 'Electronic Communications' bodies - one dealing with competition, economic and social policy issues; the other with content regulation.

A final point on regulating the Internet comes from the responsibility of Government to safeguard its people and national assets. There is growing concern that Governments are ill-prepared for the threats of '**information warfare**', computer crime and 'cyber-terrorism' as nations become increasingly reliant on the Internet and other electronic systems in every aspect of life. In the USA, much attention is being given to these issues (e.g. by Congress). In the UK, the debate is starting to develop through professional institutions such as the IEE and BCS, and a Cabinet Committee is also concerned with vulnerability of IT infrastructure (e.g. to the 'millennium bug').

MAINTAINING THE DEBATE

Internet commerce interacts with many programmes in government, between governments, within international organisations, and within national and international business. In the UK, DTI's Information Society Initiative is central and brings together such programmes as 'IT for All', the ISI Programme for Business, and the 'Enterprise Zone'. DTI acts within the EU, and is also the conduit for UK input into current discussions in the OECD on common approaches, while the UN is also involved via the UN Commission in International Trade Law (UNCITRAL) and WTO. UK industrial views are now being developed through such bodies as the Alliance for Electronic Commerce. At the European level, the lobbying over the Copyright and Liabilities Directives by Internet and Telecoms providers on the one hand and by publishers and content providers on the other, is particularly intense. Meanwhile the Internet also has the potential to transform the relationship between the citizen and the state as well as the way in which public services are organised and delivered[3]. All these aspects of electronic government provide much material for parliamentary scrutiny.

Parliamentary Copyright, 1998. *(Enquiries to POST, House of Commons, 7, Millbank, London SW1P 3JA. Internet http://www.parliament.uk/post/home.htm)*

3. For example, POST's reports "Information Superhighways" in 1995 and "Electronic Government" in 1998.