E-Policy Principles

A policymakers guide to the Internet

What is this for?

As part of the UK online strategy the Government is committed to making the UK one of the world's leading knowledge economies. Our approach is to provide an effective light touch regulatory regime in which those in the UK may engage in e-commerce and use the Internet safely and securely. It is essential for growth and inward investment that the policy framework ensures consumer confidence and trust in e-commerce and use of the Internet.

We are already updating existing legislation and regulation to facilitate electronic communication and data storage through the work of the Modernising Our Laws for the Information Age (MOLIA) Group. But we also need to look forward and ensure that any new proposals:

- do not hinder e-commerce
- can work effectively in the e-world

The Principles set out below are designed to make you aware of the impact that local, national, European and other international policy decisions and legislative proposals may have on e-commerce.

Who is this for?

This document is addressed to all policy makers working on proposals that affect or have the potential to affect the Internet and e-commerce.

Summary of the Principles

1. Always establish the policy consequences for e-commerce
   When evaluating your proposals, consider what the impact on e-commerce will be. Consider how the electronic world may add value to what you are trying to achieve.

2. Avoid undue burdens on e-commerce
   A Regulatory Impact Assessment will assess the costs and benefits of a proposal including the implementation costs to business. In considering the costs, options for compliance and impact on business, consumers and other end users, it is important to take into account the special features of e-commerce.

3. Consider self and co-regulatory options
   To encourage trust and fast, effective resolution of problems, the Government is pursuing a policy of promoting co-regulation between providers, users and regulators.

4. Consult fully on e-commerce implications
   As with any policy decision or legislative proposal, early consultation with the relevant stakeholders is essential.

5. Regulation should be technology neutral in its effects
   The effects of the offline and online regulatory environments, including the criminal and civil law, should be as similar as possible. There may be occasions when different treatment is necessary to realise an equivalent result.

6. Check that your proposals are enforceable in an electronic age
   Regulation and legislation must be enforceable to be effective.

7. Take account of the global market place - the EU and international angle
   Regulator regimes need to be reviewed and reformed at the international as well as domestic level to ensure they provide for e-commerce.

8. Consider the implications for e-Government
   Where any policy change involves the delivery of public services or other activity, you should consider at the outset how this might be done electronically.
What is so special about e-commerce?

The growth of e-commerce and the Internet is unprecedented - in the UK sales worth nearly £57 billion were made over the Internet in 2000 and, 33 million people were reported to be using the Internet in mid 2001. Here is an indication of the volume of information held and transmitted electronically in 2001: over 10 billion e-mails are sent daily; 14 million domain names are registered under the five most popular top-level domains; and the Internet search service, Google, claims to search more than a billion unique locations of web page information.

E-commerce is meant in this paper to cover any activity which involves the exchange of information across electronic networks whether within an organisation, between businesses, between business and consumers or between public and private sectors, whether paid or unpaid. This includes electronic transactions, usually the sale or purchase of goods or services, whether between businesses, households, individuals, governments and other public or private organisations and conducted over the Internet or other computer-mediated networks. The goods and services are ordered over those networks but the payment and ultimate delivery of the good or service may be conducted on or offline.

Policy makers need to be aware of some special features that characterise e-commerce and the Internet and the critical effects they may have on the practicalities of regulating these activities.

i. **Improved access to information**
   - Reduces barriers to effective communication previously imposed by geographical boundaries and time zones
   - Demolishes many existing market barriers and transforms existing business models.

ii. **Information transactions are largely placeless**
   - In which jurisdiction did the activity or transaction take place? And what is the applicable law? Internet sites owned by a UK resident (business or individual) can be hosted anywhere in the world.
   - Cross border trade can raise issues for taxation and consumer protection.
   - Alternative Dispute Resolution (ADR) can offer consumers low cost, user friendly ways of settling contractual disputes e.g. European Extra-Judicial Network (EEJ-Net).

iii. **Mobility and location of business processes**
    It is easier for e-commerce businesses to relocate to other jurisdictions if the regulatory burden gets too high. Business processes and records such as payroll and personnel operations, call centres, customer records and transaction systems, may be located anywhere in the world, or moved according to factors such as time of day, work load.

iv. **Pace of change**
    The rapid pace of technological change makes it dangerous to make assumptions about what is and is not practical when developing technology neutral proposals.

v. **Scope for cybercrime**
   - Safe and secure e-commerce relies upon authentication that guarantees the parties to a transaction are who they claim to be.
   - Tools are available that guarantee the integrity and confidentiality of e-commerce transactions so the data is not accidentally or deliberately corrupted and not read by anyone other than the intended recipient.
   - Effective network security and information security can prevent hacking, and unauthorised access to private and personal data, and minimize the risk of virus attacks.

vi. **Illegal content**
    Due to the nature and scale of the Internet, an Internet Service Provider (ISP) normally has no knowledge of the content of information uploaded or posted by its customers to websites or chatrooms it hosts. Indeed, the E-Commerce Directive requires that Member States should exempt mere conduit providers from liability, and limit the liability of ISPs for information stored on their systems, as long as they do not have actual knowledge of any illegal content, or if they do become aware of it, they remove it rapidly. ISPs operate a voluntary system of "notice and takedown", whereby if put on notice that a customer or third party is using its network to host illegal or potentially illegal content, the ISP will be advised to remove that content. However, where the ISP originates, or selects or modifies
the information on its site, it may find itself solely or jointly liable for any illegal or defamatory content.

**How do I use these Principles?**

The *Principles* have been developed to help policymakers think about what they need to take into account to consider the challenges and opportunities that e-commerce presents. You should make use of them throughout the policy process i.e. when you are first thinking about a policy proposal, as part of your on-going work, when making recommendations for action and when monitoring and reviewing the policy.

The impact of your proposal on e-commerce should be considered alongside other impact assessments and carried out at the start as an integral part of the *Regulatory Impact Assessment* (RIA) process - also see *The Policymakers' checklist*. These *Principles* will also be referred to in the guidance on the RIA process when it is revised.

The *Principles* will be kept under review, learning from lessons as they evolve e.g. from the MOLIA group. They will be formally reviewed every 2 years.

**The Principles**

1. **Always establish the policy consequences for e-commerce**

When evaluating your proposals, consider what the impact on e-commerce will be. E-commerce@its.best.uk set out the foundations for successful e-commerce, including a competitive and innovative environment underpinned by a light touch regulatory framework and clear taxation policy.

Look out for any impact your proposals may have on *Internet access* issues, for example. Network capacity and transaction speeds are important issues for effective working of the Internet as a medium for e-commerce. Be aware of any policy consequences that may impact on the speed or performance of networks. For example, might they:

- increase the amount of traffic carried by a network (including mobile devices)?
- have an adverse affect on the roll out of technological infrastructure e.g. cabling or broadband?
- have implications for the storage of electronic communications?
- make it difficult to enforce the necessary security and performance requirements?

What is the impact of lack of access on the usefulness and effectiveness of your policy?

Also, assess the impact of your proposals on both service providers and consumers. Check that e-commerce can be conducted in a secure way in compliance with data protection law so that consumers and businesses feel confident using it.

Furthermore, consider how the electronic world may add value to what you are trying to achieve. Take advantage of the functions and facilities of the "e" world rather than simply making electronic what would previously have been done in a paper-based fashion.

Considering the implications of your policy proposals in the electronic world will help you to identify the parties to be consulted and the issues you will need to raise with them (see Principle 4).

2. **Avoid undue burdens on e-commerce**

A *Regulatory Impact Assessment* will assess the costs and benefits of a proposal, including the implementation costs to business. In considering the costs, options for compliance and impact on business, consumers and other end users, it is important to take into account the special features of e-commerce (see IV above). Such as, if your policy places new requirements on business, does it have a disproportionate impact on e-commerce? E.g. are you proposing business to business
transactions that require paperwork, or proposals which affect the international competitiveness of UK e-commerce? Remember e-commerce operations can readily be moved outside the UK if the regulatory burden gets too high.

3. Consider self and co-regulatory options

To encourage trust and fast, effective resolution of problems, the Government is pursuing a policy of promoting co-regulation between providers, users and regulators. The Government sees its role as defining goals from a public interest perspective and ensuring that there is an adequate and up to date framework of law where necessary. Wherever possible it looks to those closest to the market, both providers and users, to implement agreed goals through non-legislative arrangements, such as codes of practice, guidelines and voluntary schemes for dispute resolution. These generally provide a more rapid and flexible means of responding to changing market needs, and achieving international consensus, than is possible through legislation. But you should not presume that self/co-regulation is a cost free option.

Examples:

**The Internet Watch Foundation** (IWF) (set up to combat child pornography) is an example of self-regulation, which is being copied internationally. Whilst the IWF has no legal force it provides an effective mechanism for the removal of illegal sites on UK servers and the removal of similar sites on foreign servers through the appropriate enforcement agencies.

**The t-Scheme** is an example of co-regulation. The Government is addressing security concerns raised by e-commerce encryption through industry co-operation. Industry set up this scheme in 2000. It consists of member representatives from banks, telecommunications and consumer interests etc. and has developed an approval mechanism for trust service providers. Government has been working closely with the t-Scheme, but retains the option under Part 1 of the **Electronic Communications Act 2000** to introduce a statutory regulation scheme should this initiative not succeed.

4. Consult fully on e-commerce implications

As with any policy decision or legislative proposal, early consultation with the relevant stakeholders is essential - see **Code of Practice on Written Consultation**. Indeed you may find it valuable to informally consult a selection of organisations before developing proposals further and embarking on formal consultation. It is worth taking time at the outset to ensure that you have correctly identified a full list of interested parties. For example, in addition to the relevant regulatory authorities e.g. Office of Fair Trading, Financial Services Agency, OFTEL, (OFCOM in due course) and the traditional business community, including small businesses, your proposal may impact on consumers, disabled people, ISPs, portal operators, content designers or providers and network operators (see illustrative list at Annex A). Where you think there may be an e-commerce angle, the Office of the e-Envoy can help and should be consulted.

5. Regulation should be technology neutral in its effects

The effects of the offline and online regulatory environments, including the criminal and civil law, should be as similar as possible. There may be occasions when different treatment is necessary to realise an equivalent result. In any end to end transaction, policies must be capable of spanning the media mix, e.g. an order may be placed via a website, be subject to process chasing via a call centre and advice on good delivery requested by text message.

E-commerce and the Internet are not unregulated wildernesses. National, European and international legislation applies to both the online and the offline worlds. Some legislation may have to be updated and additional legislation may be needed to secure ensure the legal integrity status and certainty of e-commerce electronic communications and the technology neutrality of legislation (examples of the latter include the **Electronic Communications Act 2000** and the **Regulation of Investigatory Powers Act 2000**).
Where a proposal is directed to the offline environment, it is important to take account of any effect it may have in the electronic context. Bear in mind that change in the electronic world tends to be much faster than in more traditional environments - scenario thinking may be helpful. You should ensure that as far as possible new proposals do not introduce legislative, regulatory or other barriers that make it more burdensome to operate electronically. Where additional regulation is necessary, it should be commensurate with the levels of risk it seeks to address.

6. Check that your proposals are enforceable in an electronic age

Regulation must be enforceable to be effective. You should be aware of the Enforcement Concordat, which sets out the principles of good regulation. Take account of the special features of e-commerce (see IV above). Make sure that your proposals are compatible with EU and UK legislation and policies of other departments. Take a look around the Office of the E-envoy and DTI websites for relevant information and sign posting.

Although e-commerce does not always respect international boundaries, domestic legislation does. When evaluating your proposals consider whether they are intended to apply to those resident within the UK and/or those resident outside the UK. National provisions may not be able to control online services and particularly the development of or access to internationally produced content.

For Europe, the E-Commerce Directive enshrined the country of origin principle - since a website is accessible worldwide it makes sense to regulate the provision of that service in the state where the provider is based. This means that any UK enforcement arrangements will not be effective for incoming online services. It also creates UK enforcement responsibilities for outgoing UK online services with effects on other member states. It is therefore particularly important to ensure that regulations that would apply to overseas suppliers are drafted clearly and concisely. Monitoring and enforcement are crucial elements of any policy.

Remember to check that e-commerce can be conducted in a secure way in compliance with data protection law. The eighth data protection principle (Schedule 1 to the Data Protection Act 1998) sets out conditions where personal data is to be transferred from the European Economic Area to a third country. It must not be transferred unless the destination country has in place adequate safeguards for the rights of data subjects. In practice, very few countries have been deemed to meet the requisite standard. The USA and the EU have entered into “Safe Harbor” agreements, which regulate the uses to which personal data emanating from the EU can be put.

7. Take account of the global market place - the EU and international angle

In a number of areas, UK legislation stems from EU instruments or international agreements. Reguatory regimes need to be reviewed and reformed at the international level to ensure they provide for e-commerce. The ability to change domestic policy may be restricted by EU and international obligations and policy options. Policy makers should apply these Principles when coordinating or developing EU and international regulatory or co-regulatory approaches on online or offline issues.

Some EU legislation or international agreements are designed to eliminate barriers to electronic ways of working. Policy makers need to be aware of two measures in particular:

- **E-Commerce Directive**
  This Directive has wide implications for the development of national e-commerce legislation. It is due to be implemented by 17 January 2002. It helps define the circumstances under which intermediaries are exempt from liability for third party content. Contact DTI for more information on this Directive and other EU legislation forming part of the EU's legislative framework for e-commerce, including copyright, electronic signatures, distance marketing, and place of jurisdiction.

- **Transparency Directive**
  All new national legislation that could possibly introduce constraints on e-commerce needs to take account of the requirements this Directive. The Directive applies to “information society services” - services supplied at a distance by electronic means and at the individual request of a recipient of services. Member States are obliged to notify to the
Commission proposed technical regulations in draft and then observe a three-month standstill period before the regulation is made or brought into force. DTI administers the notification procedure and provides guidance to Departments. See ( ) for contact details.

In the wider international arena, take account of OECD and UN e-commerce initiatives. In particular, OECD has developed policies on consumer protection, security and authentication, taxation, trade policy and market access, and competition which should be considered in developing regulatory policy.

The United Nations Commission on International Trade Law (UNCITRAL) has also been active in the area of electronic commerce and has adopted the UNCITRAL Model Law on Electronic Commerce. This Model Law has largely been reflected in the Electronic Commerce Directive and the Electronic Communications Act 2000 but departments should be aware of it.

8. Consider the implications for e-government

The Principles above address the effect of policy decisions and legislative proposals on e-commerce in the wider economy. In addition, where any policy change involves the delivery of public services or other activity, you should consider at the outset how this might be done electronically. Where new regulations, monitoring or other transactions within government are proposed these must be e-enabled by 2005. So, for example, they should not embed restrictions such as requiring paper copies or signatures without considering the cope for using electronic signatures and authentication procedures.
ANNEX A

ILLUSTRATIVE CONSULTATION LIST (ref Principle 4)

1. Regulatory Authorities

   OFTEL
   Office of Fair Trading (OFT)
   (OFCOM)
   Information Commissioner

2. Business including small business

   Confederation of British Industry (CBI)
   Alliance of electronic Business (AeB)
   Federation of Small Businesses (FSB)
   Small Business Service (SBS)
   Institute of Directors (IoD)

3. Consumers

   Consumers Association
   National Consumer Council

4. Disabled

   RNIB

5. Communications Service Providers

   ISPA (Internet Service Providers Association)
   LINX (London Internet Exchange)

6. Portal operators

   MSM
   Yahoo
   AOL

7. Content designers

8. Content providers

   BBC
   Banking e.g. Egg.com
   Retail e.g. Tesco.com

9. Network operators

   BT
   ntl