



## CONSUMER PROTECTION ISSUES IN ELECTRONIC COMMERCE

### Introduction

This paper examines the consumer protection issues that have to be resolved if the EU in general, and the UK in particular, is to be the location of choice for global electronic commerce activities by both large and small businesses and if the equivalent law is to apply to on-line and off-line trading.

90% of international business is now conducted electronically at some stage of the transaction. In 1998 20% of UK business transactions were electronic, but only 0.01% were over the Internet. This is set to change rapidly as consumers and small firms increasingly discover the economic advantages of electronic commerce. Consumers get more information, lower transaction costs, enhanced product customisation and on-line delivery for that which can be delivered electronically. Suppliers can bypass traditional retailers and distribution chains, giving them direct access to global markets. However, take up is being held back by widespread scare stories which are undermining consumer confidence.

E-commerce does pose some genuinely new challenges. It enables consumers to purchase from a remote, and maybe unknown, location which is not under human control during the course of the transaction, opening up new possibilities for errors, flaws and fraud. Consumers require a level of certainty which gives them confidence in the process used, the bona fides of the apparent trader, and the underlying security of their data and their money. Little new law is needed in the UK, which already has strong relevant legislation, most of it applicable to electronic commerce with only minor amendments. Much can be achieved at a technical, design or marketing level if there is a requirement to do so - whether stemming from self or statutory regulation or market forces.

Over-protection could be as damaging as no controls at all since it would drive electronic business offshore. The consumer is probably no more vulnerable when purchasing goods or services over the Internet than when ordering goods by telephone for later delivery, having already paid by credit card. It is not possible to remove all risk from trading, but consumers can, and should be, alerted to those risks.

### Recommendations

1. The UK should take the lead in creating an environment in which it is good to do electronic business and which inspires consumer confidence world wide. Achieving this will require co-operation between government and the business community as well as involving consumer organisations.
2. The same law should, as far as practical, apply on-line as off-line. Specific measures should be technology neutral and recognise that business "models" (eg the "any-to-any" Internet), as well as technologies, change.
3. HMG and EU should encourage self-regulation wherever practical. These would include domestic and international kite marking and dispute resolution procedures. These must give consumers clear information as to their rights and liabilities and be subject to effective and independent scrutiny.
4. Legislative initiatives should focus on those areas where change is essential (e.g. statutory cooling-off periods are meaningless for material downloaded on-line) or wholly new problems are created (e.g. in English law you cannot deceive a "machine").
5. The EU should be consistent in how it addresses the issue of jurisdiction and applicable law in its legislative initiatives, particularly with regard to enforceable redress for consumers purchasing across national borders. Both HMG and the EU should be active in global debate on these issues.
6. All relevant bodies should promote widespread e-consumer education.

## Regulatory Principles

Those wishing to enhance confidence in the Internet as a medium for achieving economic benefits are concerned that regulations which increase cost or reduce choice will drive electronic commerce “off-shore”, out of the reach of EU jurisdiction, helping neither consumers nor EU-based suppliers.

The “light touch” of self-regulatory codes is favoured where ever practical. Their application and effectiveness must be closely monitored and any deficiencies remedied in order to achieve the level of confidence envisaged. Those applying such codes in specific markets (sector or national) must also be able to co-operate, globally if necessary, to maintain and promote overall consumer confidence.

Some argue for a single regulatory framework, promoted and administered by an alliance or partnership between service providers and consumer organisations, which can act as a focal point - perhaps in partnership with Government (co-regulation). They claim that the component parts of such an “On-line Trust Foundation” already exist.

Others, including many users already subject to statutory regulation in their off-line markets, regard such a unitary approach as impractical

because their state regulators (e.g. those for Financial Services - from consumer credit or insurance sales to personal savings and investment), in the US as well as EU, are already applying their off-line rules to those selling on-line into their regulated markets.

There appears to be consensus on the need for rationalisation and co-operation (between both self-regulators and statutory regulators) with regard to the promotion and policing of codes of practice with compliant Internet web-sites easily identified by “seals” or trust marks”. Such co-operation needs to be international and to cover the security of transactions, data protection and privacy and warranties and redress procedures.

It is critical for business confidence that consumers know about the regulatory regimes and see them as effective. A structure that meets management objectives is not much use if the customers stay away!

The requirements applicable to Codes of Practice for Internet based trade involving consumers are discussed in Appendix 1. They do not necessarily apply to business to business electronic commerce conducted under well-established procedures and it is important to ensure that new initiatives do not impact these accidentally.

## Market Solutions

Business prefers market solutions to additional consumer protection regulation or legislation and believes this can best be achieved by the promulgation of good practice through example and by competition. Buyer-driven good practice is seen to be essential if potential customers are to move from browsing to buying. Those wishing to promote e-commerce (suppliers, traders and governments) must therefore be seen to be taking consumer protection seriously, including funding and other support. Government and industry should also actively promote consumer education, particularly by their own example. EU Governments and the Commission could do more to demonstrate confidence and best practice by their own use of electronic commerce than by legislative initiatives.

Protection, including checkable information and security of payment, has a cost. Perceptions of the need for such protection (including the role of Trusted Third Parties to authenticate transactions and guarantee payment between those who have never met) vary according to the nature and location of the transaction, supplier and consumer as well as the value. Moreover “trust is earned”, by those who live up

to their word, meeting their obligations, whether or not the technology works or their trading partners meet theirs. “Trust” is rarely conveyed by licensing, whether by Government or Trade Association, save where the licensing body is seen to build a track record of credibility, including the acceptance of liability for the consequences of its actions and of its decisions not to take action.

Banks, credit card companies and notaries are developing a variety of new electronic authentication, authorisation and payment protection services, based on existing “trust” frameworks, many of which already make extensive use of secure global electronic communications networks, in the expectation that these will be covered by the same regulatory frameworks and statutory liabilities as for the traditional paper-base equivalents. Meanwhile some e-commerce product and service suppliers see a need for lower cost, self-regulatory, solutions and wish to limit the liability of participants to enable increased competition. There are legal moves in the United States (proposed new Commercial Code) to limit the default liability of software and service providers. There is also strong lobbying on the part of Telcos

and Internet Service Providers regarding their liabilities for the traffic they carry.

Given the volume of international trade that is already conducted electronically, albeit commonly via structured EDI and secure e-mail

rather than the public Internet, it is important that any proposed changes to traditional regimes be rigorously assessed for their potential to disrupt well established and effective methods without giving commensurate consumer benefit.

## Kite and Trust Marks

Codes of practice (see Appendix 1) must provide sufficient protection to build and maintain consumer confidence. This entails cost-effective avenues for complaint resolution and effective promotion and policing to exclude and expose rogue traders. Realistic penalties are needed for non-compliance with codes of practice as well as effective deterrents for bad practice (e.g. spamming - unsolicited and irresponsible commercial e-mail).

Widely - ideally, universally - recognised seals or trust marks are needed to indicate which merchant's websites comply with which *clear* sets of standards, rather than merely implying approval by a responsible body. The technology is becoming available for trust marks to be mounted on the "browsers" used by consumers to alert them as to whether sites are accredited. Trust marks are particularly important to engender confidence in SMEs and in lesser

known brands, but need the support of major brands in order to ensure universal acceptance.

A recent survey in the USA found that 70% of kite marked traders were not complying with the relevant codes of conduct. This underlines the need for schemes to have routines for effective action against non-compliance (by those who have subscribed) and against "passing off" (by those who have copied the mark with little or no intention of compliance). The UK Government's statement (White Paper "Modern Markets: Confident Consumers" of 22 July 1999) that it is working with the Alliance for Electronic Business, the Consumers' Association and the Office of Fair Trade to set up a new body to accredit electronic commerce codes which guarantee security of payment and privacy of information, identified by digital hallmarks to deter unauthorised copying, is therefore an important initiative.

## Consistency

The overall objective is that consumers using electronic commerce will have a level of protection consistent with other forms of commerce. They should be neither advantaged nor disadvantaged. Attempts to use the harmonisation of e-consumer protection across the EU to "pull through" in other areas break this principle and could well be counter-productive. In broad terms, what is bad practice or illegal off-line should be bad practice or illegal on-line.

However, as off-line laws vary so widely between nations (within the EU as much as globally), there will be difficulties in achieving these goals. There cannot be consistency both across the Internet and between on-line and

current off-line law at a particular location.

Self regulation schemes do not necessarily have to be confined to participants within a single legal jurisdiction and can therefore help achieve some level of international consistency. Rules and standards for entry to a self-regulation scheme must be clearly identified through trader best practice guidelines. *Governments can give a lead here by the public acceptance of best practice for all their own transactions.* Information about existing advisory and regulatory bodies should be accessible electronically, via a help button or hotlink, *as well as* physically (postal address and phone/fax numbers).

## Dispute Resolution

Consumers need confidence that enquiries and complaints will be dealt with at least as fairly and effectively as for traditional trading methods, although it may not be feasible (or useful to the consumer) to use the same processes. The objective must be an equality of outcome.

Suppliers should provide information on accessible, affordable and effective routes for redress and the procedures for the resolution of

disputes where available. These should avoid the expense of involving courts or regulators. Authoritative and recognised ombudsman procedures, with cost-effective routines for handling cross-border dispute resolution are the ideal. Suppliers should also monitor their own performance on meeting customer expectations, including response and resolution times for customer complaints, and take remedial action where necessary.

Initially policing procedures tend to be passive, responding to customer complaints rather than actively seeking out breaches, but visible. effective, fast and enforceable sanctions against rogue traders are essential for codes to acquire credibility. It may be, however, that the active encouragement of whistle blowing by competitors as well as consumers will also be needed to test and publicise procedures and to secure acceptance and credibility on all sides.

The routes for redress must be easily identifiable (both within states and cross-border), reliable and

rapid and with clear and achievable procedures. These could include:

- the existing customer service measures of the trader;
- the trade association of which the trader is a member;
- an independent self-regulation scheme set up to control a market sector;
- statutory measures, both national and international.

## Jurisdiction

There are well established rules on applicable law for international business to business trade. These have led to three broad approaches for physical cross-border commerce:

- shipping so as to comply with the law of the country of destination (assumed by most existing legislation and by the participants in the G8 discussions on electronic commerce);
- shipping “free on board” under the law of the country of origin (leaving the recipient to comply with all local documentary, fiscal, etc requirements before the goods can be released at their destination);
- doing business under an agreed contract which specifies the applicable law and location for the adjudication of disputes (e.g. Islamic Law adjudicated in London).

Many of the small firms being encouraged to sell over the Internet have never before sold their products and services across national boundaries. Some believe the growth of e-commerce will depend on their being able to sell overseas under the laws that apply in their domestic markets.

Meanwhile many of the consumers now being encouraged to buy on-line have never bought abroad other than as tourists making purchases to bring back as personal imports. They are unaware just how different are the consumer protection laws of neighbouring states within the EU, or the different legal implications of giving authorisation to charge either your credit or your

debit card. The issues become more acute as the digital TV “couch potato” goes “seamlessly” on-line to the web after clicking the TV zapper on an advert and moves “equally seamlessly” from the “protection” of the UK Advertising Standards Authority and Independent Television Commission to ...?

Attempts to “harmonise” within the EU on issues which are outside the remit of the US Federal Government are likely to be counter-productive. Rapid progress within current international forums is unlikely, given the slow progress on long-standing problems on responsibility for action on international telecoms fraud.

The growth of mass-market international e-commerce is more likely, therefore, to depend on contract-based frameworks which apply the expertise of the global freight-forwarding industry (largely centred around Heathrow). This already handles the physical delivery of high value goods ordered over the Internet from well-known US ICT suppliers. We can see global parcels operations beginning to look at low-cost services for small firms.

There is also, however, a need for much greater support for and attention to the work of organisations such as SITPRO (Simplification of International Trade PROCedures) in the UK and radical improvement in the interfaces for documentation, including for VAT, between EU Customs and Tax authorities.

## Legislative Initiatives

The Internet blurs established concepts of legal boundaries but the rights of consumers vary considerably between nations. It is important that both trader and consumer know what laws apply to the transaction they are considering. The problem of location provides an opportunity for the UK to be seen by the world’s consumers as the place where problems can best be resolved. Little additional legislation is required within the UK to meet the needs of consumer protection in electronic commerce.

Consumers and suppliers will soon find existing laws and taxes catching up with them when they trade electronically. Governments were willing to turn a blind eye to personal imports while they were low volume, but now they are becoming too big to ignore. This gives added urgency to the need for solutions to the current policy logjam on applicable law(s) and jurisdiction(s). This will be the subject of a separate EURIM Briefing.

## Codes for Electronic Commerce

The concept of self-regulation requires the formulation of a set of rules to which those being regulated adhere. Such codes already exist in many of the sectors now engaging in electronic commerce and some of these can readily be adapted or extended to make them relevant to on-line transactions. Other organisations are attempting to create new codes. There are suggestions that various "umbrella" codes should be created in an effort to bring consistency to this burgeoning field, but because of the complexity of any large organisation's activities and relationships it may already be too late to achieve this.

The advantages of codes to the trader are that they stand in place of additional law, they can be tailored to the needs of a particular sector, competitors are subject to the same costs and liabilities, and publicising the fact of adherence to them is good for business.

The advantages of codes to the consumer are that they provide a measure of certainty in a confusing area, they identify individual traders as meeting certain standards and - when backed by self-regulation with enforcement procedures - they are a means through which redress can be obtained if a transaction goes badly wrong.

Codes for electronic commerce should

- be based on and linked into the equivalent codes for physical commerce (e.g. the UK Codes of Advertising and Promotion);
- make it clear what standards (including any specific legislation) are being complied with;
- require controls safeguarding the security and privacy of all information provided by users (including credit card and other payment authorisation details), unless they give *express* permission for other uses.
- include accessible, effective and independent routes for the resolution of

disputes, which are, as far as possible, also capable of operating on-line.

They should also require the display, before contract formation, of clear and concise information covering:

- identification of the supplier - legal name, address, country/state of establishment, main physical business address, e-mail address, telephone and fax numbers, hours of business with reference to time zones;
- any registration/ licensing information (e.g. VAT number) required for physical trading;
- the goods and services to be delivered (including itemised descriptions in sufficient detail);
- price (including delivery charges and applicable taxes, or "free on board");
- delivery arrangements (including expected time scale);
- payment arrangements;
- guarantees, process for obtaining warranty (if any) and after sales support (if any);
- information on consent and commitment (including cooling-off periods if applicable);
- routines and policy for the cancellations of orders, returning products, refunds;
- complaint and redress procedures and other significant terms and conditions;
- membership of relevant trade organisations and contact details for validation;
- the jurisdiction under which the contract is made and subsequent disputes will be settled;
- privacy statements covering the use and sharing of any personal information being gathered, *before* such information is requested.

---

In the current debate, codes are being referred to interchangeably as "Codes of Conduct" or Codes of Practice", which is adding to confusion. It would be well to return to the traditional distinctions. A *Code of Conduct* should relate to principles and generalised standards of behaviour. A *Code of Practice* sets out in some detail the way in which a particular group will operate and Codes of Practice will vary significantly between sectors and over time. A multi-national company may well derive a single Code of Conduct for electronic commerce but will probably need a different Code of Practice for each jurisdiction in which it is located. *Best practice* is achieved through the day-to-day methodical and appropriate implementation of the codes by all parts of an organisation.

## EURIM Briefing No 27

### APPENDIX 2

*This paper has been prepared by a member of the e-commerce working party as a discussion draft and comments on it and further ideas are invited prior to its distribution as an independent briefing. Please send your observations to the working party rapporteur, Emma Fryer. (fax: 0171 631 1164; e-mail: emma.fryer@geo2.poptel.org.uk)*

### The Problem of Location

At the heart of much of electronic commerce's regulatory challenge lies the concept of location. The debate currently rages about whether the ruling location should be that of the seller (the source) or of the buyer (the destination). But this debate ignores the vital prior question of whether there is a way to determine in a reliable manner the actual location of either of the parties to a transaction. Should there prove to be no suitable mechanism for this, it would become pointless to pursue further the debate on source versus destination. The technology of the Internet currently appears to offer little comfort in this regard. These notes explore the reasons.

In the tangible world, we blithely assume that we can resolve the question of location and usually we can. Letters have return addresses and confirming post marks and telephone numbers include area codes. In truth, those tangible-world indicators may not be as reliable as they at first appear. For example, a telephone number may re-direct to a call centre located almost anywhere; we may post an order while travelling; we may call from an anonymous pay-as-you-go telephone. However, what we buy by these means is almost invariably tangible - we must give a delivery address and those in authority can observe the delivery process. But most importantly, cross-border purchasing is rare and it takes considerable effort and intent to circumvent the normal location indicators.

The Internet is quite different in that it routinely fails to reveal physical location. Moreover, there are techniques and services, which Internet users have at their disposal, which positively aim to conceal identity and location. However, there are technologies waiting in the wings which could operate to give certainty to indications of location, but their acceptability to Internet users is unproven. In what follows, we try to disentangle the central issues.

All the electronic packets of information which transit the Internet contain addresses. These addresses are number sequences, similar to

telephone numbers, which uniquely identify the sender and receiver. On the face of it these numbers, known as IP addresses, should serve unequivocally to locate both parties to a communication. Unfortunately this is not the case for a number of reasons:

- An IP address need not be assigned permanently to a particular person or computer in the way that numbers attach to telephone lines or to mobile handsets. It is normal for an IP address to be "borrowed" from a pool only for the duration of a connection session to the Internet. This typically applies to the user side of a transaction much more often than to the supplier side but can apply to both.
- Many access the Internet by way of Internet Service Providers (ISPs). They connect to their ISPs via conventional telephone connections. The IP address which appears in a given transaction belongs to the ISP's location and provides no indication of the location of the end user. There is nothing to stop a user in one territory telephoning to use the services of an ISP in another territory.
- Many a business chooses not to operate the equipment which supports its Web site on its own premises. It is much more economical to employ the hosting services of a specialist. The business's Web site is on the specialist's equipment and uses an IP address appropriate to the specialist's location. This may or may not be in the same territory.
- There are Internet services now in operation which deliberately act as intermediaries between the buyer and the seller in order to maintain the anonymity, and hence the location, of the buyer.

Of course there are cases where an IP address does belong uniquely to a buyer or to a seller and this IP address can reveal a location. But this is far from saying that all IP

addresses reliably reveal location because this is simply untrue for all practical purposes.

It is worth noting that almost invariably a buyer contacts a seller not via a numeric IP address but by a more meaningful character string known as a Universal Resource Locator (URL). An example is "www.microsoft.com". The internal mechanisms of the Internet convert this behind the scenes to the corresponding numeric IP address. Many of these URLs contain a geographic designation as in "www.dti.gov.uk" where the final "uk" indicates the United Kingdom. Similarly "fr" indicates France and "de" indicates Germany. Unfortunately, this indication fails any reliability test because there is nothing to stop a business using non-geographic URLs, particularly those ending in "com". Moreover, even a URL giving geographic indication may silently re-direct to a location in another territory.

How can we resolve this issue? Various ideas have emerged which purport to reveal location much more reliably. However, all attract considerable criticism as to their practicality.

Tangible goods which demand physical delivery provide little challenge. The delivery address defines a location. Whether this is the true ultimate location of the buyer or just a forwarding address is not a problem unique to electronic commerce since it applies to all distance selling. The problem relates to digital goods and some financial services which involve, or may involve, no contact between buyer and seller other than electronically across the Internet.

One suggested system invokes the payment instrument as the means of revealing location. So, since most current transactions use a credit card and there is a billing address attached to every card and to every card acceptor account, those who clear the credit card transactions could declare the known locations. The theory is good but the practice is much more complicated. The presumption that on-line links exist around the world to make all this possible in real time is simply wrong. Credit card operators are unlikely to volunteer to pay for the implied investment. In

any case there are issues of protecting personal data which might block the whole approach. And of course there are a variety of existing intermediary services and proposals for new anonymous payment instruments - say, cybercash - which may become very popular in response. On balance, this approach is unlikely to succeed.

A second suggestion is the universal use of mutually recognised digital certificates - the electronic equivalent of personal identity cards - all locked into place by a global Public Key Infrastructure (PKI) which would authenticate everything. Only those buyers and sellers who could provide authentic digital certificates would be able to participate in transactions. Again this is good theory but hopeless practice. The time and cost attached to constructing such a PKI would be quite beyond anything which the IT industry has ever undertaken. We can surely expect its implementation to take many years before it reaches sufficient scale to be effective. By which time, electronic commerce will have developed without it. It is fruitless to pursue such a massive and risky scheme even if governments were prepared to pay for it.

The conclusion has to be that:

- the basic technology of the Internet itself is not capable of revealing a reliable indication of location;
- current and likely facilities built on top of the Internet generally make it harder rather than easier to detect location; and
- there is no practical system on offer which will reverse the trend to anonymity in the foreseeable future.

In summary, those who wish to legislate based on territorial location will have to find non-technical means to achieve this and be prepared to accept that individual buyers will be able relatively easily to conceal their true locations when this suits them. The alternative is to seek ways of regulating and taxing which do not rely on location and its reliable determination.