

---

# Legal & Regulatory Update

## *Alastair Tempest*

*has been director general of the Federation of European Direct Marketing (FEDMA) since 1999. He has made his career in European public affairs strategy and commercial communications policy.*

## A question of trust and confidence — Self-regulation of e-commerce

*Alastair Tempest*

*Received: 15 December 2000*

### Abstract

Concerns over the erosion of consumers' trust and confidence in e-commerce are being expressed by industry, governments and consumers alike. Consumers complain that fulfilment is often very slow; that they do not always have details to contact e-merchants (or do not get a reply); that financial transactions are not secure; and that their privacy is intruded upon by software tools which they either do not understand or cannot remove.

To help restore trust and confidence requires a sophisticated series of measures — the use of trustmarks, codes, alternative dispute resolution systems (ADRs) and consumer complaints systems and privacy-enhancing software. FEDMA proposed the package of measures outlined in this paper as its contribution to solving some of the major concerns.

**Keywords:** e-commerce governance, delivery commerce, privacy, European Commission/European Union, trustmarks, codes and alternative dispute resolution systems (ADRs), FEDMA (Federation of European Direct Marketing)

As more and more users are attracted to the Internet, and the services available become ever more complete, more global and more complex, the challenge of how best to regulate the Web becomes pressing. We are told by research that although more users are buying goods or (more commonly) services online, there is a serious increase in lack of confidence and trust among 'netizens'. How can we redress the situation, and protect both consumers *and* business investment?

There are a number of elements in addressing this key question which make e-commerce particularly difficult and unique. First, it is the first global medium, and there is no way that the enormous variety of laws, regulations, or even codes of best practice can be applied evenly worldwide. There is not even a global body able to complete a basic legal framework. The nearest could be the World Trade Organization, but at present the WTO has no mandate to consider the issues.

Second, the issues raised are so complex that they defy any simple solution. In 1999 the International Consumers body undertook a study of the problems. Their findings have been repeated by many other studies at worldwide, regional and national levels. The concerns of users can be summarised as delivery, privacy, and financial security. Of these the problems of 'd-commerce' (delivery) are probably the most obvious and yet the most intractable. Non-delivery of purchases or other problems connected to d-commerce may, possibly, be the basis for the poor

Alastair Tempest  
FEDMA,  
439 Avenue de Tervuren,  
Brussels B-1150,  
Belgium  
Tel: +32 2 778 99 20  
Fax: +32 2 778 9924  
E-mail: atempest@fedma.org

performance of most companies and therefore a key to the lack of trust and confidence identified by research.

The failure of d-commerce was obvious to experts in direct marketing years ago. In a study for the European Commission started in 1995, FEDMA identified d-commerce as the source of major problems. It does not give any satisfaction to say 'we told you so', but what is deeply worrying is that solutions seem as far away now as they were in 1995. The problems include late or non-delivery of products; difficulties in establishing contact with the seller; failure to get money back for returned products; extra costs (particularly postage and taxes) not clearly stated in the purchase price; lack of information on the rights of the purchaser; and frustration at a lack of an independent clearing house for complaints.

**Experts are in short supply**

None of these problems is new for mail-order experts, who have specialised in overcoming such difficulties for years, but the problem is that such experts are in very short supply, and many e-commerce sites have been set up by entrepreneurs with excellent ideas and products, but no concept of the logistics of direct marketing.

Concerns over privacy can probably be solved more easily, but again, in a very fast-moving technological and communications world the abuses of the overenthusiastic or greedy have created major problems which must be addressed. The great spam epidemic may not have reached European users to the extent experienced in the USA, but it is ever present in the debate in Europe; the use of tracking cookies, of harvesting e-mail addresses from Internet chat fora, and the perception of the 'porous' nature of the Web in general create a feeling of unease. Society has, after all, become used to the concept of the anonymous shopper. It is difficult to return to the idea that the business from which one buys should know and remember what one has bought, or, indeed, even have an interest in ensuring that I, the consumer, remain a client. We have been conditioned by years of mass media advertising to have very little loyalty to either what we buy, or where — both being conditioned mainly by what promotions caught our eye and our geographical location.

However, one thing we were sure of was that we could use credit cards with a pretty good chance of not being charged for purchases we did not make. Stories in the press about hackers carrying off thousands of credit card numbers, and the lack of physical 'contact' on the Internet between buyer and seller, have resulted in a vast increase in the number of queries (American Express said that about half of the queries it receives now are related to Internet purchases).

For regulators these problems reinforce the desire to impose laws, but the question is how and where?

The inevitable reaction is to reach for the national law book, or at best for regulations at the European Union level. This has resulted in additional restrictions, often based on the concept of 'country of consumption' or 'country of destination' control,<sup>1</sup> although the main thrust of EU legislation still remains based on the country of origin control (the country in which the business is established<sup>2</sup>).

The reaction of national courts to the Internet has tended towards national control of content (for example the AOL cases in Germany and

France, which were both eventually overthrown, and the recent case of France against Yahoo!<sup>3</sup>). Although we should not draw too close a relationship between content liability and commercial communications, there are clear parallels which raise concerns for the future. So far national authorities have been remarkably tolerant of the Internet. If this changes, an army of national authorities could descend on operators to demand changes, challenge practices, or seek to apply damages. The various national laws on data protection in Europe alone could create serious problems for operators if they were all applied with full vigour and in the most restrictive manner.

The time has therefore come to ensure that both operators and users have a set of rules to work with and a system to ensure that complaints are dealt with fast and effectively.

In April 1999 FEDMA presented a paper to the G8 Group on e-commerce, in which it was pointed out that the complexities of a global medium for marketing (advertising, selling, informing and retaining customers) needed a sophisticated self-regulatory approach. This was called the 'Ring of Confidence'.

The Ring of Confidence foresees a combination of a code, privacy policy statement, trustmark (guarantee seal), consumer complaint resolution mechanism (CCRM), alternative dispute resolution system (ADR), verification and authenticity systems, privacy-enhancing technologies (PETs), effective action against cybercrime, and education of both the consumer (the user) and the operator (e-commerce merchant/eBusiness).

FEDMA argued that it is practically impossible to control all commercial activities on the Internet. However, consumers should be able to identify easily the bona fide e-merchant, and should be left in no doubt that *caveat emptor* applies when dealing with marketers who are either not well-known brands or do not subscribe to recognised trustmarks/codes.

There is already no lack of organisations — official, 'non-profit-making' (such as trade associations), or commercial — which offer trustmarks, codes, etc. This, in turn, can create additional confusion, and therefore the work of both the Federal Trade Commission (FTC) in the USA and the European Commission towards defining criteria for acceptable codes/trustmarks, etc, is essential. Such work is also going on in the OECD, which has adopted guidelines on specific issues such as data protection.

There is a debate on whether or not accreditation of codes/trustmarks could be a solution. A system, TrustUK, has already been set up by the major players in the UK with the blessing of the UK government. We shall have to see if this can be translated on to the European or even global levels.

In its code of conduct<sup>4</sup> FEDMA took into account all the relevant European legislation,<sup>5</sup> main European codes (EuroCommerce (retailers) and Mail Order Traders), and the national direct marketing codes on e-commerce (Finland, France, Spain, Switzerland and the UK). It is hoped that this code will become a model for other bodies, either to adopt as it is or to adapt to their specific sector requirements.

**Need to define  
criteria for  
acceptable codes  
and trade marks**

A support for codes can be achieved via software solutions (often known as PETs — privacy-enhancing technologies — although not all are directly related to privacy *per se*). PETs come in many different forms, from the privacy preference policy developed some years ago by the World Wide Web Consortium (W3C), to filters, privacy pop-up boxes, software to make the user anonymous, and cookie identifiers. Within this category, FEDMA would add the e-mail preference service developed by the US DMA which allows consumers not wishing to be sent unsolicited e-mails to register and be removed from e-mail marketing lists.

FEDMA is now working on a trustmark. This is more difficult, in that four national direct marketing associations (DMAs) already have well-established trustmarks (Guarentia, Spain; TrustUK; L@belsite, France; and JurisNet e-confidence, Switzerland). Ideally FEDMA would like to see a common denominator being accepted which could also be extended to non-DMAs and, indeed, outside Europe. This could be either an element in a trustmark, or an overlay for trustmarks. Such a development would guarantee that the codes behind the trustmark contain common elements (given the need to reflect national regulations, we cannot expect that a standardised code is produced, nice as that would be).

An element of the FEDMA code requires a customer complaint resolution mechanism (CCRM) to be on every website. It is remarkable to see how many websites fail to provide even an e-mail address. FEDMA's proposal is to produce a template or model CCRM, with a multilingual facility which can be used to allow customers to communicate their complaints to the e-merchant in their own language, and have a reply. We are convinced that the vast majority of complaints are easy to solve, but that if they are not solved fast, they quickly become major concerns which, in turn, lead to a loss of trust and confidence.

Some complaints, however, will not be solved between the e-merchant and its customers. The OECD,<sup>6</sup> European Commission<sup>7</sup> and Global Business Dialogue on e-commerce (GBDe) have all proposed alternative dispute resolution systems (ADRs) as a solution. ADRs offer mediation for disputes. The European Commission is also setting up a network of official bodies (consumer ombudsmen, fair trading offices, etc), called EEJ Net, to provide dispute resolution handling.

Another area where work is progressing is in verification and authenticity. Verification systems allow buyers to check the e-merchant with whom they are doing business. At present these are available for business to business via Identrus (a combination of banks worldwide) and the International Chamber of Commerce among others. Authenticity systems include digital signature, keys, intermediation by a third party, etc, to ensure security of transactions.

One task for the authorities, which FEDMA feels extremely necessary and yet is largely ignored, is cooperation and effective prosecution of cybercrime.<sup>8</sup> While self-regulation for the mutual benefit of both consumer and business can be highly effective, it will never give pause to those intent on cheating the consumer. It is already possible to identify certain serial cybercriminals who operate scams, pyramid sales, etc worldwide. There are also the organised crime syndicates who use the Net

**A customer  
complaint  
mechanism on every  
website**

for their various criminal activities. The problem, FEDMA believes, is that official concern has concentrated on the latter and left the smaller crimes unchecked. There is no doubt that major crimes need to be solved fast, but the scams and frauds which take a couple of hundred dollars here and there are far more likely to undermine the trust and confidence of individual netizens. This will have, in the end, a major negative impact on the vast majority of honest e-merchants.

Finally, everyone agrees that there is a serious need for education of both the user (consumer) and the e-merchant on how best to benefit from e-commerce. As suggested at the beginning of this paper, major problems are caused by transactional issues and logistics. These are areas crying out for better training. The user also needs to be properly informed as to what can reasonably be expected from e-commerce, why certain software is in place and what it is intended to do (such as cookies), and which trustmarks are to be relied upon.

In the past, consumer concerns about certain business practices have taken relatively long periods to materialise. We are now in a communications evolutionary process which is so fast that problems and concerns arise almost instantly. It is said that there are seven Internet years in every one calendar year. Problems therefore appear far faster, and finding solutions becomes a race against time.

The industry must work closely together to find these solutions. The trustmark/code/ADRs systems around the world are now organising an informal network. This is good, but much more needs to be done, and done fast. For one thing is absolutely certain — if we lose the consumer's trust and confidence there will be no e-commerce except business to business, and even that could suffer from a general malaise of lack of trust and confidence.

### **References**

1. Proposals from the European Union on the country of applicable law (Rome Conventions); country of jurisdictions (Brussels Regulation), and unit trusts (USITs). All at present proposals.
2. EU Directives on Data Protection (1995) and E-Commerce (2000).
3. In the first two of these cases the question was did the access provider (AOL) have control over what messages were posted on chat fora, but the most recent case concerns a website accessed via Yahoo! which sold Nazi memorabilia and propaganda contrary to French law.
4. Adopted 5 September 2000.
5. EU Directives on Distance Selling, Misleading and Comparative Advertising, and E-Commerce. The Data Protection Directive encourages industry sectors to negotiate codes of conduct, which FEDMA is currently undertaking with national data registrars.
6. The OECD held a meeting on ADRs in The Hague on 11–12 December 2000.
7. The European Commission has a 1998 recommendation on ADRs which it is currently reviewing.
8. The Council of Europe is now working on a convention on cybercrime and expects to complete its work in 2001.