E-Commerce. Consumer protection proposal for improving the protection of online consumers

Salaun, Anne

Published in:
Computer Law and Security Report

Publication date:
1999

Document Version
Publisher's PDF, also known as Version of record

E-COMMERCE

CONSUMER PROTECTION – PROPOSALS FOR IMPROVING THE PROTECTION OF ONLINE CONSUMERS [1]

Anne Salaün

This article aims at proposing better solutions for the protection of consumers on the Internet while increasing consumer confidence in E-commerce. Today, consumer protection remains regulated by traditional rules not specifically devoted to the online world which do not address specific issues raised by the electronic environment. The proposals described in the article are addressed to Web site owners and official authorities who are both concerned to establish a trustworthy and secure online environment.

The general scope of application of consumer protection rules set forth in the European set of laws raises the question as to the effective protection of consumers in the online environment: are consumers equally protected when contracting on the Internet than when contracting in a 'traditional' environment? Consumers legitimately expect to see their interests protected in a similar way, be they involved in an electronic transaction or in a 'traditional' one. The absence of any specific protection on the Internet brings to light some uncertainties as to the situation of the individual consumer in relation to online advertisers, online providers, and more generally to online professionals. This situation is strengthened by the fact that electronic commerce weakens the position of consumers, more than traditional distance sales: the international character of the network, the electronic character of the means of communication used, the rapidity for concluding a contract. Together this means a totally different method of buying goods and services at a distance, where the consumer is placed in a situation never faced beforehand.

Electronic commerce is challenging the rules providing for protection of consumers with regard, *inter alia*, to commercial communications and contracts concluded at a distance: new questions are arising as to the applicability and effectiveness of traditional rules in the online environment. The digital marketplace produces new difficulties, confronting consumers with a new range of specific problems.

The current legislation ensuring a mesure of protection of consumers at the European level, relevant to the digital marketplace, is mainly the following: the *Distance Contracts Directive*[2] — one of the major measures providing protection to consumers when the latter conclude a contract at a distance, including on the Internet. Although this text is not particularly devoted to electronic contracting, it brings important provisions ensuring, among others, that reliable information is provided to the consumer, both before and after the conclusion of the contract; that a right of withdrawal allows the consumer to renounce the contract without penalty and without giving any reason; and that the performance of the contract takes place within a reasonable period. This Directive has been completed by a draft Directive on distance financial services, adopted on 14 October 1998.[3]

A European Recommendation on *Electronic Payment Instruments*[4] states that the holder of a payment instrument is no longer liable when the instrument has been used without physical presentation or electronic identification of the instrument.[5] This major improvement in the holder's liability is aimed at ensuring that issuers promote only secure payment instruments where risks of fraudulent use are minimized. The absence of any constraining impact of the *Recommendation* should not weaken this provision: it should definitely be seen as a new policy within the European Union.

A Council Resolution on *the Consumer Dimension of the Information Society*[6] acknowledges, on the one hand, the impact of the new technologies on the daily lives of the citizens, including possible risks that can be suffered and, on the other, the potential advantages consumers can get from the new Information and Communication Technologies. The Resolution also stresses the necessary provision of an *equivalent protection* regarding the new technologies: consumers should not feel less protected on the Internet than on the offline world.

The preamble of the Council Resolution makes reference to the *OECD Ministerial Declaration on Consumer Protection in the context of electronic commerce*, written on the occasion of Ottawa Conference held in October 1998. Although, as expected, no Guidelines for Consumer Protection in the context of Electronic Commerce were adopted, the Declaration stands apart by promoting initiatives from the private sector: the necessary tools for ensuring confidence in the digital marketplace should be developed by businesses, apart from any legislative action.

The latest legislative initiative at the European level is the *Proposal on certain legal aspects of electronic commerce in*

ISSN 0267 3649/99/$20.00

the internal market[7] where consumer protection is dealt with. The Proposal raises, among others, the issues of commercial communications distributed through the network, electronic contracts and applicable law. This text is a first step towards specific protection of consumers on the Internet.

Beside these different pieces of legislation, it is quite obvious that the business sector itself has the incentive to seek a safe and trustworthy environment where consumers are confident to contract. Initiatives should therefore not only come from the legislature but also from the business sector. Furthermore, in the light of the OECD Declaration practical measures should be adopted aimed at better taking into consideration the consumers' interests.

The discussion below focuses on the areas where improvements could be brought and addresses some solutions that might lead to a better awareness of the position of the consumer in the online environment. The analysis is obviously not exhaustive, but tries to address a general point of view of the consumers' expectations with regard to electronic commerce.

The article tries to follow the different stages of a commercial transaction: the receipt of commercial communications, the identification of the provider, the pre-contractual steps, the formation of the contract, and the post-contractual steps. Then issues are addressed at a more general level such as Web site labelling as a way to give preventive solutions and alternative dispute resolution in case of litigation.

COMMERCIAL COMMUNICATIONS

Spamming and right of opposition

The new means of communication gives rise to new types of consumer canvassing for commercial purposes through the E-mail address of the consumer. Providers get E-mail addresses in newsgroups, mailing-lists or throughout the Web and take advantage of the low costs of the network to bombard either the newsgroups or individual E-mail addresses with messages, mainly for commercial purposes.[8] This technique has important consequences for consumers since the frequent sending of messages can lead to a blocking of the network and represents downloading costs born by consumers.

This situation is quite unbearable for holders of an electronic address, who feel helpless to prevent the receipt of such messages. Still, a right to oppose the receipt of messages for commercial purposes is admitted in three European Directives: first, Directive 95/46/EC *on the protection of individuals with regard to the processing of personal data and on the free movement of those data*[9]. Article 14-b urges Member States to grant the data subject the right "to object, free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing". Second, Directive 97/66/EC *on the processing of personal data and the protection of privacy in the telecommunication sector*[10] states that unsolicited calls for purposes of direct marketing should not be allowed either without the consent of the subscriber concerned,[11] or in respect of subscribers who do not wish to receive such calls; and third, Directive 97/7/EC *on the protection of consumers in respect of distance contracts*: article 10 § 2 recognizes the *opt-out* principle where individual distance communications may be used only where there is no clear objection from the consumer.

Those articles clearly state that a right to oppose unsolicited receipt of commercial communications should be granted to the consumer, and that this right should be available free of charge. As a matter of fact, some spammers do facilitate a reply message to their spams notifying the recipient's wish for the removal of one's address. This is by a simple return E-mail message, but such examples are few.

How could this right of opposition be enforced?

The effectiveness of a right of opposition presumes however the existence of a mechanism allowing consumers to make known to providers their position regarding unsolicited commercial communications. First, information to consumers on the availability of such mechanisms is expected. To be fully efficient, an opposition mechanism should be centralized and should enable providers, before sending any message, to have access to E-mail lists where the wish of the consumer not to receive commercial communications has been clearly stated.[12]

Practically, the opposition mechanism could be materialized in two different ways:

- the first commercial communication sent to the consumer should contain information about the possibility of refusing the receipt of such messages, and on the steps to take in order to implement this. In this first hypothesis, the duty to inform the consumer would rely on the *author of the communication*;

or

- when the E-mail address is granted, the *access provider* should inform the consumer of the right offered to him to oppose unsolicited commercial communications received via his E-mail address. The duty of information falls here on the Internet Access Provider. At the request of the consumer not to transmit commercial E-mails to him, the IAP would be empowered to filter such messages as soon as they arrive at his own mailbox. This would prevent the consumer from receiving those messages, costs of receipt and downloading being avoided.

This possibility to filter commercial communications should be read in accordance with the *Proposal on E-commerce*. Article 7 states that an unsolicited commercial communication by E-mail should be "clearly and unequivocally identifiable as soon as it is received by the recipient". With such a principle, how would the consumer be able to filter a commercial message before it arrives in his mail box? Article seven could have been better drafted by stating that a commercial communication should be identifiable as soon as it is *sent* by the service provider. Such a wording would open the possibility to offer filter services by allowing an identification of the commercial aim of the message as soon as it is sent. A third party would have been able to filter the messages on behalf of the consumer, the commercial communications would have been stopped before reaching the recipient's mailbox.

The above-mentioned distinction concerns solely the information that the consumer possesses on the opposition mechanism and about his right to subscribe to a list to be

ISSN 0267 3649/99/$20.00

removed from commercial communications. Another step is the concrete functioning of the list: the question remains as to the monitoring of the list by a specialized body. Should it be a public body or a professional body gathering different categories of providers? Whatever the choice is, it should at least avoid a situation where an increasing number of opposition lists are put to consumers. This would certainly weaken their purpose.

Moreover, the existence of opposition lists should match with consumers' wishes. The list should offer enough opposition categories (i.e. opposition to all types of commercial communications; selected opposition to identified providers or to categories of providers, etc.); and should make sure that the finality of the list is not diverted and re-used for commercial purposes.

Privacy concerns[13]

Positive synergy between privacy protection and consumer protection

Privacy issues meet consumer concerns when the personal data disclosed during a transaction are potentially useable for illegitimate purposes by Web site owners. The above mentioned 95/46 Directive participates in the protection of consumers on the Internet since the protection set forth for every data subject is applicable to every consumer.

Basically, on the grounds of this Directive, personal data[14] may only be processed provided one of the following conditions is met: either the processing is necessary (it can be necessary for the performance of the contract, for the compliance with a legal obligation, for the protection of vital interests of the data subject, for the performance of a task carried out in the public interests, *or for the purposes of the legitimate interest pursued by the controller*) or the data subject has unambiguously given his consent.[15] The rights provided to the data subject are the right to be informed, the right of access and the right of rectification.[16]

Privacy issues participate towards the protection of consumers on the Internet. As explained above, consumers benefit from article 14-b — the right to oppose, free of charge, the processing of personal data for marketing purposes. Likewise, the rights of information, access and rectification allow consumers to monitor the use of their personal data. A synergy is thus observed between the two areas of protection. Privacy concerns become consumer concerns — consumer protection taking advantage of the rules set forth to protect data subjects' privacy.

Negative effects of privacy threats to consumer protection

On the other hand, privacy threats also create a lack of protection for consumers.

First, privacy can be threatened by the ease with which data can be collected and transmitted over the network. Without any knowledge of the consumer, personal data can be collected and used by numerous actors, which "dilutes the responsibility for data security and data protection and multiplies the risk of breaches in security and protection".[17] It becomes almost impossible to control and know who is collecting the data and for what purpose. Furthermore, surfing on the Internet is not anonymous: it leaves traces enabling a consumer profile to be developed from the steps followed by the consumer on a commercial Web site.

Another major concern for consumer protection is linked to the use of 'cookies', used by Web sites to collect and process personal data. *Cookies make use of user-specific information, transmitted by the Web server onto the user's computer so that the information might be available for later access by itself or other servers.*[18] Cookies are used to set up consumption profiles and send targeted advertising. Despite the possibility offered to the consumer to choose whether he agrees or not to receive cookies, the question remains as to the enforcement of the principles set forth by the Directive. The cookie does not mention either the controller of the data, or the purpose of the processing.

Threats can also arise from invisible processing. Advertising banners placed on Web sites (e.g. on search engines like Yahoo or AltaVista) are often adapted to the consumer's search. As soon as the consumer enters a keyword, the advertising banner presents a product in relation to the keyword entered in the search engine. This happens through an invisible exchange of information between the search engine and the cybermarketer; an exchange of information that is obviously hidden from the data subject.

And last but not least, the efficiency of the protection granted by the privacy Directive relies on the protection granted at the international level, and on the protection offered to European data subjects whose personal data are processed outside the European Union.[19]

Enhancing privacy protection on open networks and making the Directive's rights effective would undoubtedly enhance the protection of consumers.

IDENTIFICATION OF THE PROVIDER

Consumers are faced with the difficulty of establishing the identity and location of the provider with whom they deal, although such information assumes a great function of confidence and trust in consumer's mind. There is a great difference with traditional commerce where the businesses they contract with are easily identifiable and whose reputation is clearly established. Furthermore, the identification of the provider should be emphasized in an international environment. In this field, the labelling of the site can be a great help for consumers (*see infra*).

Confidence could also be reached through the references of the provider in a *trade register*. This is foreseen by article 5 (d) of the Proposal for a Directive on Electronic Commerce: the trade register in which the service provider is entered and any registration number in that register should be disclosed to the recipient of the service. One could also imagine a hyperlink with the site of such an official trade register which would allow direct consultation.

Whenever the provider holds a digital signature, a certificate has been issued by a Certification Authority. This certificate would easily identify the provider: as the certificate is public, a link could be offered to the Certification Authority's site.

ISSN 0267 3649/99/$20.00

INFORMATION PROVIDED TO THE CONSUMER

Both the presentation of the information and its content should be strengthened in the online environment: the distance character of the contract justifies that accurate and comprehensive information is provided to the consumer before the contract is concluded, and the global network calls for a strengthening of the information disclosed.

Presentation of the information

According to the wording of article 4 of the Distance Contracts Directive, the information must be provided "in a clear and comprehensible manner in any way appropriate to the means of distance communication used". This should be understood as forbidding providers to make a distinction between categories of information by presenting a first range of information in an attractive way by using colours, animated pictures, etc., and another range of information in an unpleasant way aimed at dissuading consumers from reading them. The possibilities offered by the technique should not lead providers to hide information to the detriment of others, thus misleading consumers by dissuading them from reading the whole range of information.

Furthermore, it is important to note that such prior information should be accessible at any stage during the visit on the site: too often the information is no longer accessible once the good has been put in the 'shopping basket' even though it is important to enable the purchaser to come back to it. A link or an icon should allow a consultation of the product's information at any step of the transaction.

Strengthen the informational content: additional information and sample

The information disclosed by the provider to the consumer prior to the conclusion of the contract is crucially important since the parties are not by nature in contact with each other. This statement is strengthened by the global environment of the network — where the exercise of the right of withdrawal takes a new dimension in terms, among others, of return costs — and by the interactivity of the network where numerous goods and software, directly downloaded to the consumer's computer, often fall under an exception to the right of withdrawal.[20]

Article 4 of the Distance Contracts Directive enumerates a list of prior information provided to the consumer that should be delivered as a minimum in the online environment. When the good ordered is for 'immediate consumption' (in other words when it is directly downloaded to his computer) *additional information* should be given to the consumer. Such information must enable the consumer to check the compatibility with his own software, in order to avoid technical incompatibilities: a situation where goods received online are not useable for such reasons due to a lack of prior information should not be the consumer's responsibility otherwise he is left with software that can neither be exploited nor returned.

The idea of providing additional information to the consumer was developed in a first draft version of the OECD Recommendation concerning *Guidelines for the Protection of Consumers in the Context of Electronic Commerce*.[21] It states that additional information should be provided to consumers with regard to digitized goods, services and/or software ordered and delivered over the open network. According to this draft Recommendation, the information must include, *inter alia*: specific information as to the characteristics of the goods, services and/or software and the operating system and equipment requirements necessary to utilize the good, service or software efficiently; the transmission costs; the terms and conditions of any applicable software licence agreement; and any specific limitations or conditions on the return of digital information. This principle, although considerably watered down in the second and third versions of the draft recommendation, should encourage providers to provide tailor-made information according to the good, service or software delivered.

Furthermore, where the technology permits, a *sample* of the product should be sent to the consumer. We assume that for many products or software delivered online the sending of a sample, or in other words an indicative piece of the product, would not represent technical difficulties for the provider. This would, on the contrary, have the advantage of placing potential purchasers in a confident frame of mind since they would be able to receive, free of charge, a sample of the digitized good they would have been reluctant to purchase without this prior check. After receipt, the recipient will feel confident about ordering the good if it is in accordance with the characteristics described in the offer and technically compatible with his own system.

Confirmation of the information presented to the consumer

The Distance Contracts Directive provides for a duty to confirm the prior information given to the consumer. Article 5 states that "the consumer must receive written confirmation or confirmation in another durable medium available and accessible to him of the prior information, in good time during the performance of the contract". The term of *durable medium* implicitly refers to electronic distance contracts where a written document is not foreseeable.[22] One cannot expect to receive a confirmation on paper when dealing with online contracts.

One should not lose sight of the Directive's requirement: the consumer must 'receive' confirmation: the obligation weighs on the provider, the consumer needs not play an active role. For example, the confirmation would not be satisfactorily validated if the provider simply were to content himself with posting it on-screen leaving the consumer to download or print out the information.

A second important issue linked to the confirmation concerns the medium. To respond to the requirement that the medium is 'available and accessible' to the consumer, a *choice* must be made as to the medium used. Indeed, a confirmation could be available to the consumer but not accessible if the medium is not readable by his computer (e.g. a floppy disk where the file is saved in a different format). The issue of confirmation takes on a new dimension since here again the compatibility between the provider's computer and the consumer's one has important consequences. This situation finds

ISSN 0267 3649/99/$20.00

no echo in traditional distance contracting where confirmation is mostly sent through postal services, and no question of compatibility arises. It is therefore important that a choice is proposed to the consumer as to the medium through which the confirmation will be sent, taking into account his technical equipment.

Most of the time the confirmation will be sent through an E-mail, which is the easiest, quickest and cheapest way to reach the consumer. However, E-mail is not always a solution if the consumer has reached the provider from a public place (e.g. cyber-café): no personal address is attributed to him in this case. Still, if the contract has been concluded in compliance with the requirements of the *Proposal for E-commerce*,[23] it means implicitly that the consumer has been able to interact with the service provider, irrespective of the existence of a personal E-mail address. In that case it is foreseeable that the confirmation will reach the consumer through a public E-mail address, provided the service provider makes sure that the consumer has effectively received it.[24]

INTERACTIVITY WITH THE SERVICE PROVIDER

Direct contact with the service provider should be made possible. The provider should offer a hyperlink to consumers to enable them to enter into contact with him for any information request or complaint. The technology offers possibilities that should be used by professionals: an icon placed on the provider's site would offer a real interaction; questions would receive direct answers and complaints could be addressed easily.

Benefits can also be taken from the interactivity of the network with a mention of the Codes of Conduct the provider subscribes to, and possibly a direct link with the organization in charge of the monitoring of such Codes.

SUMMING UP THE TRANSACTION

Besides the great opportunities offered by electronic commerce, the risks of wrongful utilization are inherent to the technique itself. No means of distant communication up to now has ever offered consumers the possibility to conclude contracts so fast, by a simple mouse 'click'. This rapidity implies obvious risks of misuse and can lead to the formation of undesired contracts due to technological mistakes.

Requiring the consumer to honour a contract entered into after an error is not satisfactory. The consent of the consumer must be explicitly given in order to avoid a dispute as to the existence of the contract. The solution could be to present a *final summing up* of the transaction before the consumer definitely enters into the contract.

A summing up of the transaction would have the advantage of presenting to the consumer a re-statement of all his choices (characteristics of the goods/services chosen, price, delivery costs, arrangements for payment, performance, exercise of the right of withdrawal, etc.). This summary, presented on a unique page, would allow a visualization of the content of the contract the consumer is willing to conclude and, above all, it would enable the consumer to bring rectification and thus avoid mistakes due to a misuse of the technique. The consent is then given to the summing up of the transaction, leading to a clear and comprehensive summary of the content of the contract. Such a practice would bring an end to consumers, mistakes leading to undesired contracts.

It should be mentioned that the *Proposal for a Directive on certain legal aspects of Electronic Commerce* urges the Member States to act in such a way that service providers make available to the recipient of the service "appropriate means allowing him to identify and correct handling errors".[25]

In practice, many sites already propose a similar summing up arrangement before the consumer purchases the goods or services,[26] but a generalization of this practice should be encouraged.

The first draft of the OECD Guidelines imagined a slightly different system where the *consent* of the consumer must be given at *various steps*. To enable the consumer to give his consent in a clear and transparent manner, separate steps are presented to him where he can clearly express his intent to purchase the good/service. The steps foreseen are: the selection of the good or service; the agreement to the full price as stated in the offer, terms, conditions and methods of payment; the acceptance of credit options; the agreement to other aspects of the contract; and the final agreement to the purchase. This system was not adopted in the draft *Guidelines*, perhaps for practicable reasons, although a consent split in different stages would allow a clear and transparent expression of the consumer. However, as long as a clear summing up is presented to the consumer, it is satisfactory to enable the consumer to express a clear and unambiguous consent.

CONTRACT FORMATION

Contract formation is foreseen in article 11 of the E-commerce Proposal. Three different steps are envisaged before the contract is deemed concluded: (i) the first step is (obviously) the recipient's acceptance, when the consumer demonstrates his wish to conclude the contract by sending a message to the provider; (ii) the second step is the acknowledgement of receipt by the provider sent to the consumer, (iii) and the third one is the confirmation of the acknowledgement of receipt by the consumer.

Although this system seems complicated at first sight, it can, in reality be easy and fast. It brings to the consumer the advantage of being absolutely certain that the provider has received his acceptance and is ready to perform the contract. Punctuality problems are even avoided with this system, like the unavailability of a product. The provider has the chance to check the availability of a product before sending an acknowledgement to the consumer. However, article 11 could be improved with regard to consumer protection.

First, uncertainties remain with regard to the messages sent. What should happen if a message is not received by the recipient or if the recipient pretends not to have received the message? Also, what if the content of the message has been altered? It is regretful that the Commission's Proposal does not encourage the use of means guaranteeing the integrity and authenticity of the message, like the digital signature. The use of a digital signature would provide security as to the formation of the contract, although a cost is incurred from this security with the consequence that a signature might not be adapted to low cost transactions. But should one accept a

ISSN 0267 3649/99/$20.00

lesser degree of security for low cost transactions, i.e. a transaction without digital signature?

As far as consumer protection is concerned, the time of conclusion of the contract would be better chosen when the confirmation is *sent* by the consumer, instead of when the confirmation is *accessible* to the provider (the confirmation mentioned here is the message sent by the consumer confirming the acknowledgement of receipt sent by the provider). The time of conclusion chosen in the *Proposal* places the risk of a non-receipt of the message by the provider *in the hands of the consumer*, although the latter cannot be held responsible for a technical failure.

RECORDING OF THE TRANSACTION

In order to guarantee the means to prove the transaction and its content, a *recording of the transaction* should be available to the consumer from the provider. Such a record would be useful for both parties: it would identify the contract, its content, the time of conclusion, etc. It could be sent to the consumer through a similar medium than the one used for the confirmation of information, and would present the advantage of focusing on the major elements of the contract. Moreover, the parties could refer to it in case of dispute. In order to guarantee the validity and integrity of the recording, an electronic signature could be used.[27]

The idea of recording the transaction is also presented in the second draft *Guidelines for Consumer Protection in the context of Electronic Commerce*: "acceptance should be notified in a format which allows the parties to access and maintain a complete and accurate record of the contract".[28]

PAYMENT: SECURITY ISSUES

The major issue concerning electronic payment is security. Confidence in electronic commerce will only develop when security with regard to payment on the Internet is provided. Credit card number and expiry dates are too often disclosed over the network without a sufficient and reliable security system operating.

The lack of security is one of the reasons why consumers are reluctant to make payments online and thus to buy goods or services on the Internet. So long as mere communication of the apparent number on the payment instrument suffices to engage a transaction, the broad mass of electronic transactions will remain insufficiently secure, which clearly represents a brake to their development. Moreover, security is expected at two different levels: first, during transfer of the information over the network and second when the payment data is stored. In these circumstances data transmitted should not be accessible to unauthorized third parties.

EU Recommendation on Electronic Payments

The European Commission's Recommendation of 30 July 1997 "concerning operations carried out by means of electronic instruments of payment, in particular the relationship between the issuer and the holder" participates in the protection of consumers on the Internet.[29] Beside provisions on responsibilities and liability of the parties, one major input into the document relates to the limitation of the holder's liability. The holder may not be held liable for payments made without either his physical presence or electronic identification having taken place; the simple use of a confidential code, or similar means of identification, is insufficient to engage his liability. The holder is therefore not engaged by the simple communication of the apparent number of the payment instrument. The aim of this provision is to ensure that issuers of payment instruments are bound to consider the issue of security and to provide consumers with a system sufficiently secure to minimize the risks of fraudulent use of payment instruments and of payment data. Either implementation in the Member States must be achieved or, if not, the will of the Commission to adopt a constraining measure will be proposed.

Information

Consumers are entitled to receive sufficient and accurate information about the payment systems proposed. Information should describe the different payment possibilities available to enable consumers to make their choice. The security of each payment system should obviously be described in words understandable to every consumer. Reference to a security system — for example the SSL Protocol — is not enough to increase consumer confidence in payment systems as long as consumers are not able to understand the consequences of using such a system. Providers should therefore pay attention to the information provided about the technique referred to and its consequences.

Information should also focus on the related fees, charges or handling costs incurred by the use of a particular means of payment.

Charge-back

Whenever the contract is either not performed or withdrawn from by the consumer, any sums already paid must be refunded (within 30 days according to article seven of the Distance Contracts Directive). The reimbursement of the consumer in such cases has fundamental importance: consumers will be reluctant to purchase goods or services on the Internet if they have no certainty as to their reimbursement in case of non-performance of the contract or withdrawal. If they want to attract consumers, online providers should furnish reliable information and offer the assurance that any sum paid will be charged back in case of dispute.

The OECD has issued a draft Recommendation on this question of charge-back,[30] laying down principles that should be taken into account by Member States to guarantee the charge-back principle for consumers in relation to international distance contracts. The mechanism of charge-back is foreseen as a means enabling consumers to get refunds in dispute cases, thus avoiding redress mechanisms. The Draft Recommendation pleads for a voluntary based charge-back mechanism at the international level aimed at increasing consumer confidence in payment systems. Charge-back would be granted in the following circumstances: withdrawal by the consumer; invoice mistakes; fraud due to the seller; a lost or stolen instrument; non-delivery of the good ordered beyond any foreseen delay; non-conformity of the good to its

ISSN 0267 3649/99/$20.00

description, and inertia selling where a payment has been made.

Solutions could also be imagined in other instances. Consumers would feel quite satisfied with a site displaying a clear policy regarding reimbursement, where assurance would be given that any sum received by the provider (before the good is effectively delivered) would be automatically charged back in case of withdrawal or non-performance from the contract. Likewise, the sum paid by the consumer could be blocked by a third party and transmitted to the provider after the withdrawal period, unless the performance of the contract did not happen as foreseen in the contract.

Site Labelling

The principle of site labelling could be seen to be the answer to both consumers and service providers with respect to electronic commerce. Combining the technology and an audit procedure, it offers a general solution for providing trust and confidence by complying with consumer protection rules and commercial practices principles in general.[31] The reliability of a Web site owner is ensured by a seal posted onscreen, attesting the site's support to the principles set forth by the labelling company. The seal offers the possibility, through a hyperlink, to check the issues identified as most relevant by the labelling company with regard, notably, to electronic commerce with consumers.

As far as consumer protection is concerned, site labelling can be profitable by developing a trustworthy and secure environment over the Internet.[32] It should however meet certain criteria if it is to be really efficient. Labelling detractors argue that label initiatives do not particularly address consumer issues; that the co-existence of labels with a large number of other labels divert from their purpose. They also argue that labels endanger compliance with legislative texts since they are not based upon existing legislation. Such arguments should not be ignored. To provide concrete input to the protection of consumers, site labelling should be framed within minimal conditions.

At first glance, the following conditions seem important to take into account when setting-up labelling activities:[33]

- the very first objective of the label is the *information to the consumer*: the information aims at increasing consumer confidence and trust. The label should, therefore, be properly explained to consumers. All accurate information should be available in order to enable the consumer to understand the meaning and the purpose of the label. It should notably contain information on the labelling company, the criteria for granting the label, the audit report performed by the labelling company on the Web site owner. A hyperlink should make this information directly accessible from the Web site concerned;
- the label should also guarantee the *identity of the Web site owner*. As already mentioned, the identification of the site owner is a major difficulty faced by consumers when compared with traditional distance selling activity. Information provided by the label should clearly and unambiguously establish the identity of the Web site owner (this should also be seen in the light of a link to an official trade register and/or the certificate delivered by a Certification Authority);
- strict account should be taken of *existing legislation* in the fields of law covered by the label: all relevant legislation should be analyzed by the labelling company. Compliance with the legal requirements should constitute the very first commitment of any site wishing to be granted a label;[34]
- only a *limited number of labels* should be developed: an increasing number of labels placed on Web site pages would create a deep confusion and would damage their purpose and credibility. Efforts should be made to avoid a multiplication of labels: first on a geographical basis, labels should not be limited to the territory of one Member State. They should at least cover the territory of the European Union. Secondly various fields could be covered by one label: a label should not necessarily be limited to the protection of consumers, or the protection of privacy for example. Its scope should be broader in order to limit the number of labels;
- *minimal requirements* should be complied within any case. Labelling should be based on a voluntary system and should not become a compulsory standard for electronic providers. Neither should it dedicate any monopoly, be it public or private. A competitive market should be the basis of labelling activities. The setting-up of the label and the criterion to grant it should ideally be defined in collaboration with the relevant professional and consumer associations;
- the label should be surrounded with *security measures* guaranteeing that the label is not reproducible and/or usable by non-authorized parties (e.g. by a site which fails to comply with the label's requirement and/or which has not asked for the label). Such measures should also confirm that the label can be withdrawn whenever the site is found not to be in compliance with the requirements;
- *no prohibitive costs* should be charged to small or medium-sized enterprises (SMEs) willing to participate in the labelling process that would separate them from the benefits of this technique with regard to the development of a trustworthy environment;
- the labelling company should be aware of *liability issues*. It should take the necessary steps to provide for any damages arising from the label (be it for the audit report, the monitoring of the label, the relation with third parties, etc.).

ALTERNATIVE DISPUTE RESOLUTION

Member States shall ensure that, in the event of disputes between an information society provider and its recipient, their legislation allow for the effective use of out-of-court settlement mechanisms including by appropriate electronic means. The European Commission opens the door to alternative disputes resolution mechanisms in the *E-commerce Proposal* (Article 17).

Alternative dispute resolution (ADR) solutions are developed to solve the disputes arising on the network, thus contributing a mechanism designed to answer to consumers' expectations. ADR is seen as complementing judicial procedures, its aim being to propose a tailor-made solution that is better adapted to the particulars of the network compared with traditional court procedures.[35] As a matter of fact, ADR is

ISSN 0267 3649/99/$20.00

currently the most suitable mechanism for solving disputes arising between a consumer and a service provider on the Internet. The reason for this is easy to understand. As stated in the recitals of article 17 of the *Proposal*, out of court dispute settlement should be "particularly useful for some disputes on the Internet because of their low transactional value and the size of the parties, who might otherwise be deterred from using legal procedures because of their cost".[36]

ADR is seen as a means to answer consumers' fears regarding the solving of disputes. A quick, affordable solution, tailor-made to the network's particular features, fits without any doubt with consumer expectations. Be it through negotiation, conciliation, mediation or arbitration,[37] ADR presents an attractive solution and numerous advantages. Its flexibility allows an adapted procedure and an adapted solution, within a limited period of time and at low cost value. Its confidential nature is also of importance for businesses who might prefer to see their conflicts solved without any publicity. Furthermore, an alternative solution presents less difficulties with regard to the enforcement of the decision, compared with the difficult enforcement of a judicial decision, especially in an international environment. Besides, interesting initiatives are currently developed.[38]

ADR solutions should however not develop unless within a strict framework where minimal requirements are complied with notably: (i) information to the consumer: a primary range of information should include all the necessary information enabling the consumer to understand the purpose of the mechanism and its way of functioning. A second range should focus on the voluntary character of ADR and the fact that it does not prevent the parties from going to court, at any stage of the alternative procedure;(ii) the explicit consent of both parties to submit the dispute to the third party, before and/or after the dispute arises. Furthermore, consumer associations should be invited to play an active role in the setting up of ADR rules and/or in the solving procedure; (iii) the neutrality of a third party asked either to impose a solution or to advise the parties involved in the dispute; (iv) the compliance with the legal requirements as regards consumer protection.

From a Web site owner's point of view, ADR presents also quite considerable advantages. It offers consumers an alternative way to resolve disputes, adapted to their specific needs while demonstrating the site owner's commitment to take into account consumers' interests. Together with site labelling, the commitments relating to dispute resolution become a marketing strategy for service providers, to the advantage of both parties. Consumers benefit on the one hand because they find an answer to their needs in the service provider's commitments. The service providers, on the other hand, see this as a positive strategy which will undoubtedly increase consumer confidence in buying goods and services on the Internet.

The uncertainty related to the resolution of disputes arising on the Net means that the potential of E-commerce has still to be realized. The development of alternative solutions could, therefore, assist the development of electronic commerce.

CONCLUSION

"The same level of protection provided by the laws and practices that apply to other forms of commerce should be afforded to consumers participating in commercial activities through the use of global networks." This general principle is the first statement of the OECD draft Recommendation.[39] It is based on the desire to see Governments ensure that laws and practices applicable to other forms of commerce are afforded to consumers engaging in electronic commerce.

This statement should however be seen as a *minimum basis* given that the above-described proposals show that better protection can be afforded to online consumers. Answering the specific needs of consumers participating in E-commerce can lead to a tailor-made protection taking better account of their interests. The goal of reaching *similar levels of protection* should therefore be preferred, instead of limiting the effort to something less. Otherwise this could eventually discourage further initiatives designed to take account of consumers' interests on the Internet.

New forms of abuse and threats to consumer protection call for new protective rules. The protection should be adapted to meet the needs of technological evolution whereby the consumer is placed in new situations and is faced with new threats. Moreover, online providers should not lose sight of the fact that better protection of consumers on the Internet can have a positive impact on the development of E-commerce itself. An involvement in consumer concerns and the proposal of practical solutions to consumer problems is, without doubt, the best marketing strategy a Web site owner can adopt.

Anne Salaün
Researcher at CRID (Centre de Recherches Informatique et Droit, University of Namur, Belgium)

FOOTNOTES

[1]This article is written in the context of a contract with the Belgian Ministry of Economic Affairs and the CRID. However, it represents the author's opinion and is her sole responsibility.
It represents also the author's involvement in the ECLIP project (Electronic Commerce Legal Issues Platform) <http://www.jura.uni-muenster.de/eclip/>. It does not bind the other partners of the project nor the European Commission, and does not preclude any of the final conclusions and recommendations the ECLIP project will eventually reach.
[2]Directive EC/97/7 of the European Parliament and the Council on the protection of consumers in respect of distance contracts, 20 May 1997, *OJEC* L 144 of 4 June 1997. For further developments on the Directive, see: Salaün A. *Electronic Commerce and Consumer Protection*, at: <http://www.droit.fundp.ac.be/textes/consumer.pdf>.
[3]Proposal for a Directive concerning the distance marketing of consumer financial services COM (1998) 468 final: <http://europa.eu.int/comm/dg15/en/index.htm>.
[4]Recommendation of the European commission concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder, 30 July 1997, 97/489/EC.
[5]Article 6 § 3.
[6]Resolution of 3 November 1998.
[7]18 November 1998: <http://www.ispo.cec.be/ecommerce/legal.htm>.
[8]See the following site for explanations on spamming: <http://www.multimania.com/arobase>.

ISSN 0267 3649/99/$20.00

[9]Directive 95/46/EC of 24 October 1995, *O.J.E.C* L 281 of 23 November 1995, p. 30.
[10]Directive 97/66/EC of 15 December 1997, *O.J.E.C.* L 24 of 30 January 1998.
[11]The subscriber is defined in article 2 as "any natural or legal person who or which is party to a contract with the provider of publicly available telecommunications services for the supply of such services".
[12]Punctual solutions are already developed: adding the reference *'no spam'* before the E-mail address which will prevent the 'spammer' from automatically sending commercial messages.
13See for further developments Data Protection and Online Networks, Louveaux. S. and de Terwangne C.,[1997] 13 *CLSR* 234.
[14]Personal data are defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by the reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"(article 2-a).
[15]Article 7 of the Directive.The 'data subject's consent' is defined as *any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed* (article 2-h).
[16]See: *Data Protection and Online Networks, op.cit.* pp. 241-242.
[17]*Data Protection and Online Networks, op.cit.* p. 234." (...) consumers become increasingly remote from organizations which process their data. Different categories of actors intervene in the online game (mainly access providers and information or service providers) and actors have become increasingly numerous (the Internet consists of more than 40 million users throughout the world accessing more than four million Internet sites).
[18]The Internet and Privacy Legislation: Cookies for a Treat? Mayer-Schönberger V. [1998] 14 *CLSR* 166.
[19]Although the Directive allows the transfer of personal data to third countries only if the transfer complies with the national provisions adopted pursuant to the Directive, and if the country of destination ensures an *adequate level of protection* (article 25), uncertainties remain on the actual protection granted to European data subjects outside the European Union.
[20]See article 6 § 3 of the Distance Contracts Directive: unless the parties have agreed otherwise, no right of withdrawal applies for contracts concerning the supply of audio or video recording, computer software unsealed by the consumer (indent 4).
[21]OECD, DSTI/CP(98)4,April 1998, § 53.This draft has been revised two times: DSTI/CP(98)4/REV1 and DSTI/CP(98)4/REV2.
[22]The durable medium should be heard, notably, as an E-mail, a floppy disk, a CD-ROM, a tape (audio or video).
[23]See article 11 "Moment at which the contract is concluded".
[24]That is to say the confirmation should not be sent after the consumer left the place. In other words, the service provider should be able to make the difference between a personal E-mail address and a public one that can be used by several persons.
[25]Article 11 § 2 of the Proposal.The former version of the Proposal of September 1998 was going further as it laid down that insofar as the recipient made an handling error *and* promptly informed the service provider of this error, the contract was not concluded (former article 11 § 2).
[26]See for example the Belgian virtual supermarket <www.ready.be>: the consumer visits the online supermarket, selects the products and fills a shopping list.The content of this list is accessible all over the transaction and can be modified up to the consumer's wish.The final consent is given to a visualization of this shopping list.
[27]See Electronic Signatures: another step towards a European framework for electronic signatures: the Commission's Directive Proposal, Julia Barcelo R. and Vinje T., [1998] 14 *CLSR* 303.
[28]Paragraph (31).
[29]*OJEC* L 208 of 2 August 1997 p. 52.
[30]OECD Draft Recommendation on charge-back mechanisms, DAFFE/CP(97)13.
[31]See Secure Internet Commerce: a Benchmark for Trustworthy Commerce,Wright B., [1998] 14 *CLSR* 265.
[32]Site labelling is already developed in the United States notably with the *WebTrust* initiative.This experience is developed jointly with the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Chartered Accountants (AICPA):< www.icca.ca>A similar initiative also exists in the field of privacy protection:Truste : <http://www.truste.org/>.
A similar experience is currently developed in Europe with Coopers & Lybrand: in collaboration with Belsign, a Belgian Certification Authority, they have created a seal called Trust^2. This seal is based on the compliance with the relevant European legislation in the fields of consumer protection, privacy, trade practices, intellectual property rights,VAT, etc.
[33]See also 'AGORA Consommateurs' initiative of the Belgian Ministry for Economic Affairs, Rapport de l'atelier "*Commerce Electronique : vers la confiance* !!", Poullet Y. and Royen J., pp. 57-71. <http://www.agora98.org/>.
[34]Labelling activities should not be seen as a substitute to legislative action: on the contrary, it should be seen as a complement to any legal development.
[35]The only statement that alternative solutions are being developed to solve disputes should give rise to a debate on the role of the judicial public service and its duty to propose a service adapted to the developing technologies.
[36]Although alternative dispute resolution solutions can be forbidden in consumer contracts: see the French legislation where the 'clause compromissoire' in consumer contracts is forbidden.
[37]*Negotiation* is the most basic form of disputes resolution as it is any form of discussion between the parties, with no third party intervention. In the opposite, mediation, conciliation and arbitration call for the intervention of a third party, but at different levels. In the *mediation* procedure, the third party — a mediator — is voluntarily asked by the parties to analyse the dispute, but he is not granted with any power (neither to give an opinion nor to impose a solution). In the *conciliation* procedure, the role of the third party goes further by advising the parties on the reasonable solution of the dispute. *Arbitration* is the most advanced procedure as the arbitrator has not only the power to advice the parties but to impose his decision.
[38]*CyberTribunal* where both mediation and arbitration are proposed: <http://www.cybertribunal.org>.Online Ombudsman Office: <http://128.119.199.27/center/ombuds> Other links can be found at: <http://www.osu.edu/units/law/jdr/jdr-links.html>.
[39]DSTI/CP(98)4, point 27.