http://www.droit-technologie.org

présente :

THE CYBERCONSUMER'S PROTECTION

Cristina COTEANU
Avocat
ccoteanu@philippe-law.be

25 juillet 2001

Introduction: Cyber Consumer Law - Issues and Trends

Cyber consumer law can be defined as a complex set of rules and principles relating to a multitude of substantive legal areas such as privacy, contracts and professional rules in the context of virtual space. The "Cyber Consumer" framework is completed by the enforcement of law in these areas. This underpins the protection of the cyber consumer and requires the application and enforcement of principles and rules which stem from traditional consumer law. Cyber consumer law is based on the interaction between a subordinated national law and a co-ordinated international law. This concept goes beyond any idea of cyberspace being a separate legal order. John Perry Barlow has written that *"digital technology is also erasing the legal jurisdictions of the physical world, and replacing them with the unbounded and perhaps permanently lawless seas of Cyberspace. In Cyberspace, there are not only no national or local boundaries to contain the scene of crime and determine the method of its prosecution, there are no clear cultural agreements on what crime might be*"[1]. We can infer from Barlow's theory that cyber consumers are deprived not only of the most basic principles of protection but also of any possibility of recourse to their national legal system if their rights in this area are not upheld. According to Barlow, the existence of cyberspace creates a legal "disorder" which does not necessarily rest on the creation of the rule of law but only on *"an unbounded and perhaps permanently lawless…"*[2] Today the emergence of cyberspace law gives little credibility to Barlow's theory. The concept of cyberspace is intrinsically linked to the notion of a legal order. Cyberspace is not an autonomous international space, nor is it separate from existing legal jurisdictions.

Cyber consumer law is becoming an increasingly important element today in the protection of privacy, contracts and applicable law within the framework of co-existing national systems.

At the European Union (EU) level , Articles 153 § 2 of the Treaty of Amsterdam stipulate that *"Consumer protection shall be taken into account in defining and implementing other Community policies and activities"*. Through its endorsement in this Treaty, consumer protection has gained acceptance and legal recognition within the framework of *"an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured"*.

At the national level, all EU Member States are endowed with a legal framework, which ensures consumer protection and enhances consumer confidence in cross-border cyber-transactions. On the one hand, improving the free movement of goods and services in the cyberspace market contributes to EU Member States commitments endorsed in the EU Treaties. On the other hand, the current legal framework has been adopted by these states in order to comply with European Union directives, as well as with OECD and WTO guidelines, UNICITRAL principles and the Council of Europe's efforts to harmonise laws designed to ensure an international level of protection and an active and confident consumer participation in Cyberspace.

Countries have enacted a wide range of laws, rules and regulations encompassing all stages of business-to-consumer (B2C) e-commerce. These offer protection to consumers from fraudulent, unfair and misleading practices. Examples include privacy and data protection, commercial communications of goods and services, contractual formation, prior information, right of withdrawal, unfair terms and conditions, payment, delivery, guarantees and after-sales services, applicable law and jurisdiction.

The purpose of this article is to explore fundamental questions, which the Internet is facing in the area of consumer protection. What legal requirements should be respected when contracting on line? Are contracts on line legally recognised? What are the consequences of self-regulation for the protection of the consumer? When legal problems arise on the Internet, who should support the cost of liability? Are the authorities of certification liable for consumer loss? What are the new solutions for consumer privacy on the Internet? Are we moving towards an approximation of the concept of privacy in Europe or towards a

[1] John Perry Barlow, *"Selling Wine Without bottles: The Economy of Mind on the Global Net",* http://www.eff.org/pub/Intellectual_property/idea_economy.article

[2] John Perry Barlow, *"Selling Wine Without bottles: The Economy of Mind on the Global Net",op.cit.*

standardised approach? How are the public and private sectors dealing with the protection of privacy? How can legal authorities enforce a law which by definition is limited to national boundaries and how does this impact on cross-border commercial communications on line? It is these questions which we shall address.

Electronic commerce raises a large number of questions to which it is sometimes difficult to formulate definitive responses. Moreover, it is not easy to assess whether challenges raised by technology are a driving force behind legislation or whether the existing legal framework is moving ahead at a faster pace than technology. What is clear is that when focusing on current consumer issues, practical solutions to questions facing cyber consumer protection should be found at an internationally co-ordinated level. The evolution of consumer protection at the European and international legal levels should result in the creation of a level playing field for cyber consumers worldwide.

Furthermore, only by increasing consumers' confidence in consumer protection law will electronic commerce generate a "snowball effect" on the B2C relationship. Consumers will participate effectively in the electronic commerce system only if respect for consumer rule is guaranteed in a concrete way. As the Internet operates on a cross-border basis with no regard for national territory, the question of which national or cross-border cyberlaw is applicable in electronic transactions remains an essential element for increasing consumer confidence in the Internet.

This article willfocus on the protection of privacy law and security over the Internet. With respect to privacy law, the first part of this article will analyse trends in current legislation on data protection which ensure the protection of consumers' privacy. This analysis will examine the implementation of principles on privacy in commercial transactions. At the same time, it will highlight consequences of these trends on the B2C relationship and it will put forward suggestions on ways in which companies could enhance trust among consumers.

The second part of this article will focus on the need for security over the Internet, on Community consumer directives and their contribution in recognising the legal value of contracts on line. While enforcement of these directives is dependent on their appropriate implementation by Member States, adaptation of national legislation according to these directives will inevitably lead to a "legal convergence", characterised by a whole host of national consumer protection laws as well as harmonised values at the European level.

We will now examine two elements that are most characteristic of the B2C relationship: (A) the protection of personal data and (B) security when surfing on the web.

A. Privacy protection in cyberspace: under the watchful eye of the law

While the right to privacy in the physical world is a generic term which lies in a diverse source of rights found throughout national and international law and in principles or codes of practice, the recognition of privacy in cyberspace requires a more specific co-ordinated legal framework, able to regulate the loss of control of consumers or companies over personal information provided in a borderless environment. Obviously the right to privacy in cyberspace encompasses a wide range of rights which range from e-mail privacy and data protection to the right to privacy in the workplace and when surfing on the Internet. As a consequence of the consumers' interest in controlling personal data which is generated, stored or processed over the Internet, a superimposing legislative framework has granted legal recognition to these rights at both national and cross border levels. For today's consumer, this legal recognition represents a considerable achievement.

When speaking about privacy in cyberspace, many other interests arise, namely those of the companies who develop online markets and deal with substantial quantities of personal information. Even if the interest of "privacy market opportunists"[3] finds its justification in the fact that privacy is recognised as a

[3] Karl D. Belgum, *"Who leads at Half-Time? Three conflicting Visions of Internet Privacy Policy",* 6 Richmond Journal of Law&Technology, vol VI, issue 1, 1999,

fundamental right consumers should be able to decide whether or not their personal data will be traded[4]. The interest of companies will inevitably collide with that of consumers in their control over personal information.

1. Protection of personal data

Use of personal data is positioned at the crossroads of two opposing methods of practice. One is in favour of the creation of the personal information market and the other is at the other end of this evolution with its' view of consumer protection. In other words, while personal data is becoming an increasingly important medium for the creation of markets in personal information, infringement of rules governing the use of this data are becoming more regulated with stricter penalties. Despite this growth in the formation of the market on personal information, which leads inevitably to a prevalence of business litigation, it is highly likely that this type of market development will become common in the future. Certainly, through the implementation of legislation on privacy, consumers' confidence in companies will increase and companies will simultaneously foster this confidence in the area of the Internet. At the same time, those industries , which have not yet adhered to a privacy policy, will shortly be obliged to provide guarantees for consumer privacy protection. Finally, in order to cover all eventualities in privacy protection on the Internet, e companies can exercise a discretionary power with regard to the processing of personal information and can insist on their right to treat such information as a business asset. The Amazon.com case[5] illustrates this. Jeff Bezos, Chief Executive Officer of Amazon, announced on 1 September 2000 *" that Amazon would reserve the right to treat personal information gathered at its site and those of its online affiliates as business assets that could be bought and sold as online properties change hands."* [6] Amazon maintains that its' 23 million customers were notified of this change of policy on privacy in line with the disclosure standards of the U.S. Federal Trade Commission (FTC). New users will automatically consent to the processing of their information when they surf the Amazon.com web site. The new Amazon vision on how to enhance trust in business-to-consumer transactions on the Internet seems somewhat ironic. Amazon is not a unique example. Toysrus.com has also recently declared its policy on the sharing of personal data acquired from users when they surf on the Toysrus site.

These trends in consumer privacy policies do not impede contradictory evolutions on the protection of privacy While these infringements of privacy may create serious concerns for consumers the processing, storage and use made of such personal data raises important revenues[7] for online companies. While the

---

http://www.richmond.edu/jolt/v6i1/belgum.htlm

[4] Eli M. Noam, *"Privacy and Self Regulation: Market for Electronic Privacy" in Privacy and Self-Regulation in the Information Age,* 1997

[5] *"What is Amazon.com's new policy?":*

http://www.amazon.com/exec/obidos/subst/misc/policy/privacy.html/103-8172023-3991815

[6] D. Gebler**,** *"E-Commerce chiefs back net privacy standards",* September 27, 2000, E-Commerce Times

http://www.gbd.org/media/articles/092700a.html

[7] *" The Internet (...) economy is estimated to grow to past the $1 trillion mark in 2001 and then to $2.8 trillion in 2003. A recent study from Ciemax-WEFA, an economics consulting group, commissioned by the Direct Marketing Association, indicated that one of every 13 jobs in the United States was the result of direct marketing sales activity, including jobs designing and selling advertising, supplying or delivering goods, and selling other support services, such as customer lists and consumer profiles to direct-response businesses. The same study revealed that direct marketing sales to consumers reached $630 billion in 1996, up from $458 billion in 1991. Business to business sales were another $540 billion in 1996, up from*

processing of personal data for direct marketing purposes can be perceived as a considerable source of unease, "transformation scenes" in consumer minds are always possible. In this line, Deloitte -research on "The new economics of transactions" *states that "One dimension of privacy issues will become economic in nature; some consumers will essentially "sell" their data to vendors and "infomediaries" in exchange for services or goods, while others who desire more privacy may elect to have a limited participation in that market."*[8]

Furthermore, growth in industry marketing contributes to direct marketing. For instance, in the UK " *direct marketing… is a major industry and (is) likely to grow in importance as it becomes more targeted, focusing on individuals' lifestyles, spending profiles and other characteristics and idiosyncrasies. "*[9] To rephrase Visconti's words in his famous movie "Il Gattopardo", "everything changes because nothing changes" - over the Internet everything changes, as everything is in an evolutionary process.

Wide ranges of private sectors are increasingly involved in the protection of personal data. For example, the health sector, banking transactions, purchases on line or registration with an Internet service provider. At the same time, a diversified legal framework was set out by the European Union by way of the 95/46 EU Directive on the Protection of Individuals with regard to Automatic Processing of Personal Data[10] and by the OECD, through their Guidelines for the protection of privacy and transborder flows of personal data,[11] as well as by the Council of Europe through a Convention on the protection of individuals with regard to procession of personal data[12]. Consequently, many countries have enacted legislation on privacy protection and companies have designed guides of ethical "business to customer" regulations to be applied in domestic as well as in cross-border electronic transactions. The main contribution of this superimposing legislation is to provide common standards for personal data protection.

Protection of personal data can be approached through two complementary ways: through co-ordinating standards and through technical regulatory standards. While co-ordinating standards are working towards the "common goal" of protecting consumers, technical regulatory standards follow on from these and complement the regulation of cyberspace by filling an existing gap in privacy protection legislation.

a) Co-ordinating standards

Co-ordinating standards for consumer data protection are primarily related to some specific area such as electronic payment systems (smart cards, e-cash,), encryption processes and contract formation. In the field of data protection, this means finding the lowest common denominators leading to fair practice vis-à-vis

---

$349 billion in 1991" S. Safier, *"Between Big Brother and the Bottom Line: Privacy in Cyberspace",* Virginia Journal of Law and Technology Association, 2000 http://www.vjolt.net

[8] Deloitte Research – *"The new economics of transactions - evolution of unique e-business, Internet market spaces,"* Deloitte Research, 2000, p3 http://www.deloitte.com

[9] Bainbridge D et al, *"Tilting the Windmills – Has the New Data Protection Law failed to make a Significant Contribution to Rights of Privacy",* 2000 (2) The Journal of Information, Law and Technology (JILT). http://elj.warwick.ac.uk/jilt/00-2/bainbridge.html

[10] The EU Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ No L 281, 23.11.1995

[11] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1981)

[12] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - Strasbourg, 1981

consumer information. Co-ordinating standards are formulated within the framework of EU directives, international conventions or are set out in OECD guidelines and codes of conduct. There is a wide range of codes of conducts with regard to the Internet. For example, the "European code of conduct" relating to electronic payments and the BBB Code of Online Business Practices [13] which is designed to guide ethical "business to customer" conduct.

Furthermore, EU directives also encourage the adoption of codes of conducts. In this sense, Article 27 of the Data Protection Directive stipulates that:

"1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.

2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.

Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives."

It is clear that through its' aim of harmonising national data protection in Europe, the Data Protection Directive will not be able to solve all the issues related to transparency and security. Even if some of these issues arise regularly over the Internet, some of them could be resolved through the implementation of co-ordinating standards incorporated in a code of conduct or guidelines. This poses other questions in terms of (1) enforcement of a code of conduct and (2) exercise of a co-ordinated policy.

(1) The enforcement of a code of conduct

The enforcement of a code of conduct is the result of a long-term process of exercise of principles in practice and includes their unanimous recognition. However, while a traditional code is the result of continuous practice and should be unanimously recognised at national and cross-border level as well as on a professional basis, an Internet code of conduct usually seems to have greater similarities to guidelines principles designed to be applied to virtual transactions. In this context, the next logical question which arises is whether a code of conduct should be recognised as having a self-executive value as long as its provisions were never invoked before a jurisdiction or used in practice. Or could it be envisaged that at some future date we might speak about the "general principles" recognised in international cyberspace law as we speak today about the general principles of international law?

Would these "general principles" be based on the OECD guidelines for consumer protection? As, for instance, laid out in the ABA Report on "Achieving Legal and Business Order in Cyberspace":

"Another potential solution is to not apply either the law of the consumer or of the merchant, and instead to apply common principles of consumer protection law that would govern all transactions that occur over the Internet regardless of the location of the consumer or the merchant. Such an approach would harmonise differing laws and establish a uniform law of consumer protection for Internet transactions. Harmonisation could occur through formal governmental mechanisms, i.e. treaties or bilateral agreements, or through less formal self-regulatory frameworks. "[14]

[13] The Better Business Bureau system and BBBOnLine http://www.bbb.org, http://www.bbbonline.org

[14] Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet

The recognition of a consumer protection code, which applies to every e-transaction, is subject to a test of strength between the virtual and physical environments. Any nonconformity to the code of conduct, which is revealed in its' interaction with real standards, would automatically penalise the potential value of the "code of conduct" by its transformation into a simple statement of intent. While the meaning of an Internet code of conduct seems somewhat different from that of a traditional code, the legal effect of such a code of conduct requires total recognition, not least in the specific domain for which it was designed.

With respect to a code of conduct relating to e-commerce, the provisions of the Directive on Electronic Commerce are very clear:

"Member States and the Commission shall encourage:

(a) the drawing up of codes of conduct at Community level, by trade, professional and consumer associations or organisations designed to contribute to the proper implementation of Article 5 to 15;

(b) the voluntary transmission of draft codes of conduct at national or Community level to the Commission;

(c) the accessibility of these codes of conduct in the Community languages by electronic means;

(d) the communication to the Member States and the Commission by trade, professional and consumer associations or organisations of their assessment of the application of their codes of conduct and their impact upon practices, habits or customs relating to electronic commerce;

(e) the drawing up of codes of conduct regarding the protection of minors and human dignity." [15]

It emerges from this provision that the recognition of these codes of conduct will, in the future, not only require assessment of their application but will also necessitate official recognition at national and at trans-border level.

(2) Co-ordinated policy

A co-ordinated policy can be conferred in Europe by the Working Party instituted by the Data Protection Directive.[16] At the same time, the Working Party can be a moderator of questions relating to the interpretation of certain principles on data protection. The role of the Working Party, as designated in Article 27 of the Data Protection Directive, is essential in establishing guidelines on e-commerce and in ensuring the protection of consumers' interests:

"*Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party"*

However some questions remain when we speak about codes of conduct relating to their self-executive force. When a conflict arises on the Internet, to what extent can the provision of a code of conduct be

---

Report of the American Bar Association ("ABA") Jurisdiction in Cyberspace Project empaneled in 1998 under the title, "Transnational Issues in Cyberspace: A Project on the Law Relating to Jurisdiction."

[15] Article 14, Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) 17.7.2000 EN L 178/13 Official Journal of the European Communities

[16] Article 29, European Directive 95/46/EC

invoked and what legal effect does it have? Are the principles formulated in national legislation endowed with a superior legal force compared to those formulated by a professional organisation? These are only some of the questions, which we need to address in order to, formulate adequate legal protection of consumers' interests.

b) Technical standards

As the law can not be a panacea for all concerns on privacy, technical standards constitute a valuable complement in the co-ordination of standards.

(1) Privacy Enhancing Technologies (PETs)

Privacy enhancing technologies (PETs) are welcomed by the data protection commissions in Europe. These are able to minimise or eliminate differences between national legislations in Europe. The idea of PETs is to protect personal identity by eliminating or reducing the use of personal data in accordance with the legal principle that such data cannot be used without legitimate reason and that anonymity must be assured. The functioning of PETs is based on the identification of an object or a subject without disclosing information on the person involved in on-line activities. Users who are concerned can insert their own identification details into a smart card based on "identity protectors "[17]and they are able to make informed decisions about the collection, use and disclosure of their personal information stored on this card.

(2) Open Profiling Standard (OPS)

Another emerging technical standard is the Open Profiling Standard (OPS) which enables the flow of personal information between Internet surfers and web sites[18]. The idea of the OPS is that users would create a profile of their personal information by completing standard data fields. Disclosure of information would then be possible only with the consent of the user. It seems that this solution already presents some disadvantages as the use of OPS may infringe the anonymity principle with users being obliged to enter personal information in a standards data field that has already been configured.

(3) Platform for Privacy Preferences (P3P)

The World Wide Web Consortium (W3C) works on the Platform for Privacy Preferences (P3P) [19]which gives users more control over the disclosure of their personal data on the Internet. The Internet service provider would inform users on their rights as regards their privacy when surfing the Internet and, in turn, the user would specify to what extent information they provide could be released. However, this technical standard also seems to present some disadvantages. These are illustrated by Mr Barry Steinhardt, President of the Electronic Frontier Foundation, when he speculated on the future of P3P: *"there are still a lot of unanswered questions about P3P and the underlying philosophy of industry self-regulation . . . If you turn*

---

[17] *"Privacy - Enhancing Technologies: The Path to Anonymity",* Information and Privacy Commissioner, Ontario, Canada and the Registratiekamer, The Netherlands, Vol I and II, 1995

[18] Netscape Communications Corporation Submission Supplemental Comments , FTC Consumer Privacy Hearings, June 1997, http://www.ftc.gov/bcp/privacy2/comments2/netscape.htm

[19] *See* W3C, *Platform for Privacy Preferences Project*, http://www.w3.org/P3P/

(P3P) on and say you want to be anonymous, you're going to be blocked from a lot of sites . . .There's a question of whether this will work or (whether) there will be a consumer revolt."[20]

However, the strength of P3P lies in its flexibility as it was conceived differently from the Platform for Internet Content Selection (PICS). While the PICS are used to regulate privacy practices through a method of complete acceptation or rejection, P3P allows more freedom of negotiation.

2. Enforcement of data protection legislation

The principles of data protection lie on the individual right to privacy stipulated in Article 8 of the European Convention on Human Rights, namely that "Everyone has the right to respect for his private and family life, his home and his correspondence". It seems clear that in a world where information technology allows the collection of personal information, the enforcement of data protection principles has to pay particular attention to safeguarding a fair balance between all rights and interests involved. The enforcement of data protection implies not only respect of duties, obligations and rights which are incumbent on parties but also requires that legislation divergences are compensated by a uniform interpretation of data protection principles.

a) What data controllers should be aware of

The Data Protection Directive lays down a number of obligations that controllers must comply with in the processing of personal data. These include the obligation to obtain the consent of the data subject for a specific purpose, to collect data for specified, explicit and legitimate purposes, to conserve data during a certain period, to respond to security criteria and to collect data which is adequate and relevant and does not exceed the purposes for which it was collected. The enforcement of these obligations, which are incumbent on the controllers, will require a uniform interpretation as well as equal implementation over the Internet.

(1) Fair and lawful processing

A controller should process the personal data in a fair way. This implies that the treatment of personal data should comply with legal requirements. It imposes the obligation on the controller to provide the data subject with adequate information about the use, which will be made of data which is collected, recorded. Moreover, the controller must respect the rights of the subject during all stages of the process. Any infringement to the obligations inherent in the process of collecting data risk the collecting process being qualified as unlawful.

(2) Collection of data must be adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed

This principle should be understood in the sense that the controller should be prepared to explain the reason for which the personal data is processed. Demonstrating that the collection of data is adequate and

[20] International Trade Administration Electronic Commerce Taskforce http://www.ita.doc.gov/ecom/menu.htm#Safe

relevant implies that the controller must be able to justify the existence of a casual connection between the data collected and the purpose for which it is acquired. In addition, the fact that "the collection of data must be (…) not excessive" signifies that the collecting process should respect a "reasonable" principle of proportionality between the quantity of data collected and the purpose for which it is processed. Moreover, the controller should collect the personal data for specified explicit and legitimate purposes and (it should) not (be) further processed in a way incompatible with those purposes. [21]

(3) Personal data must be kept for a certain period

The controller should kept the personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected.[22] This principle requires that the controller does not keep the data any longer than is necessary, that he periodically reviews the collected data and destroys it following completion of the task for which it was collected. Moreover, all Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use. This means that the controller should use anonymous data and regularly monitor personal data which has been collected.

(4) Security of processing procedures

The controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration and unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network and against all other unlawful forms of processing.[23] Due to the risk of processing personal data over the Internet, the controller should behave with diligence in these activities. For the controller, this implies - the obligation to be equipped with - - high standard computer material as well as with appropriately trained staff. Moreover, the controller should be able to undertake technical measures against imminent problems relating to security over the Internet.

(5) Obligation related to "transborder data flows "

The controller should not transfer personal data to countries which do not have an adequate level of protection.[24] Furthermore, the Directive stipulates that the adequacy of the level of protection afforded by a third country shall be assessed in the light of all circumstances surrounding a data transfer operation or a set of data transfer operations. The controllers should pay particular attention to the nature of the data, to the purpose and duration of the proposed processing operation or operations, to the country of origin and to the country of final destination. Close attention should also be paid to the rules of law, both general and sectoral, in force in the third country in question and to the professional rules and security measures which are complied with in that country.

In order to respond to the needs of the Directive on Data Protection of an "adequate level of protection", the U.S. Department of Commerce and the European Commission set out a "safe harbour" framework, ensuring that personal data flows to the United States are not interrupted. The European Commission has agreed that Safe Harbour Privacy Principles meet the Directive requirements and ensure adequate

[21] See Article 6§b
[22] See Article 6 §e

[23] See Article 17

[24] See Article 25

protection for EU citizens' personal information. Consequently, the US Department of Commerce will set up a list of companies adhering to these principles which provide guidance to European businesses.

(6) Obligation to notify the supervisory authority

A supervisory authority is responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive. These authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data. At the same time, the controller must notify the supervisory authority before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.[25] The role of the supervisory authority is to ensure the enforcement of the controllers' obligations and the respect of data subjects' rights.

b) What are the rights of data subjects?

While the Directive recognises the right of controllers to process personal data, its provisions endow the data subjects with a number of rights. The data subject has the right to be informed of the identity of the controller and the purposes for which data is collected.[26] In addition, he has a right of access to this data. This right of access guarantees the possibility for data subjects to obtain from the controller, without constraint and at reasonable intervals and without excessive delay or expense, confirmation as to whether or not data relating to him are being processed and information concerning the purposes for which this data is being used, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed. [27] Right of access also includes the right to obtain rectification, erasure or blocking of data when the processing does not comply with the provisions of this Directive, in particular when there is incomplete or inaccurate data.

The Directive stipulates that Member States shall grant the data controller the right not to be subject to a decision which produces legal effects concerning him or significantly affects him which is based solely on the automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.[28]

c) The compliance of controllers with the national law

The enforcement mechanism of the data protection Directive should avoid overlapping legislation. The Data Protection Directive is very innovative on this point. The Directive establishes that the controller is subject to the law of each Member State where it is established. In practical terms, the controllers would be obliged to adhere to the law of each country in which they are established. National law is applied to the processing of personal data where this is carried out in the context of activities where the controller is established in a particular Member State. When the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by national law. Furthermore, national law should be applied

[25] See Article 18

[26] See Article 10

[27] See Art 12

[28] See Art 15

when the controller is not established on the Member State's territory but in a place where its national law applies by virtue of international public law.[29]

Moreover, the Data Protection Directive considers that a Member State's law must apply to a controller that is not established on EU territory but "for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory" of the Member State. . In this case, it would not be wrong to consider that this provision applies when, for example, a provider of services located in the USA collects personal data from a consumer located in Belgium via the consumer's equipment (computer or telephone network).

The mechanism of applicable law, implemented by the Data Protection Directive, claims an extraterritorial effect for national legislation implementing this Directive.

B. Security as a precondition for the very existence of the relationship B2C

Surveys[30] show that few consumers are in a position to assess the effectiveness of existing online security and encryption methods. At the same time, it is very difficult to consider that technological knowledge and expertise would increase consumer confidence. Few consumers comprehend the technological characteristics of smart cards and cryptography. This means that increasing consumer confidence is a question of ensuring that transactions over the Internet can offer the same level of security as transactions made in a traditional environment. In other words, consumers should be guaranteed the same level of protection online as they are offline.

It seems that very often consumers have little awareness of their rights and sometimes do not know where to address their complaints. According to the Distance Selling Directive, Member States shall ensure that appropriate measures exist to allow a consumer the right to request cancellation of a payment where fraudulent use has been made of his payment card. This is in connection with distance contracts covered by this Directive. In the event of fraudulent use, the consumer should be re-credited with the sums paid or have them returned. Nevertheless, how many consumers are aware of their right to require the cancellation of a contract without penalty, for example, in the event of withdrawal?

Security problems on the Internet might be related to human intervention as well as to technological considerations. For example, the security breach of Barclays' online banking site seemed to be caused by the upgrading of its software. In the Safeway and Oxfam cases, a hacker managed to access the sites and to obtain e-mail addresses. [31] Problems of consumer confidence might arise directly from the Internet provider. For instance, a consumer received an extra charge after buying directly from the web of Direct Holidays. The spokesman of Direct Holidays explained that this was the result of a technical problem with the company web site. Ensuring security seems to be very complex in this area. As a spokesperson for Direct Holidays' commented: *"While we endeavour to ensure the accuracy of the content of the web site, this is a complex area."*[32]

It is clear that such examples impede the trust and confidence of the consumer in their transactions over the Internet. This requires that company web sites provide consumers with adequate information on security issues. However, key concerns are not only related to data protection but also to the necessity of providing an efficient and secure electronic payment system.

---

[29] See Art 4

[30] *"E-commerce and consumer"*- A report by the UK National Consumer Council, August 2000 August 2000 Publication reference PD40/2000 PD40/2000

[31] Ajay Patel*, "Consumer Confidence and online security",* Electronic Business Law, October 2000, p13

[32] "Extra charge after buying off the web", "The Times", December 2000

1. Consumer right for access to information

Information is the corner stone for consumer confidence and security in their transactions over the Internet. The gradual commercialisation of the Internet imposes the need for governments to inform consumers on their legal rights. It is in business-to-consumer (B2C) e-commerce that public policy needs to take a lead in providing consumer protection.

Another major problem with the disclosure of information is that consumers are unaware of what information is being provided. Following the results of a recent survey set up by the UK National Consumer Group, it seems that few consumers recognise or have seen any of the logos, online help or advice sites which have been presented to them. Consumers seem to need an intensive publicity and advertising campaign in order to raise their awareness of their rights when using the Internet.

The problems of Cyber consumers are very complex and should be approached not only from a market perspective but also by taking into account the existing rules in this area. The "Electronic Commerce Directive "[33] and the "Distance Selling Directive"[34] already provide a general framework on consumer protection.

a) Electronic contracting

(1) Distance Selling Directive

The Distance Selling Directive applies to any contract concerning goods or services concluded between a supplier and a consumer under an organised distance sale or service-provision scheme run by the supplier who, makes exclusive use of one or more means of distance communication.

Two provisions are relevant concerning the obligation to provide information to the consumer: prior information and written confirmation of information.

According to the Distance Selling Directive[36], the consumer shall be provided with information relating to the identity of the supplier the main characteristics of the goods or services, the price of the goods or services, including all taxes, delivery costs, where appropriate, the arrangements for payment, delivery or performance, the existence of a right of withdrawal, the cost of using long distance communication, the period for which the offer or the price remains valid and the minimum duration of the contract in the case of contracts for the supply of products or services to be performed permanently or recurrently These provisions therefore require businesses engaged in e-commerce to provide sufficient information on terms, conditions of sale and costs of a transaction in order to enable consumers to make an informed choice.

---

[33] Directive on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) 17.7.2000 EN L 178/1 Official Journal of the European Communities

[34] Directive EC/97/7 of the European Parliament and the Council of 20 May 1997, *OJEC* L 144 of 4 June 1997.

[35] See Article 2 § 1

[36] See Article 4

Furthermore, the Directive stipulates that this information should be clear, comprehensive and easily accessible with due regard to the principles of good faith in commercial transactions. This means that the information should be provided in such a way that gives consumers an adequate opportunity to review their decision before entering into the transaction and they can retain a record of the agreement.

Moreover, the consumer must receive written confirmation, or confirmation in another durable medium , setting out his rights and obligations prior to the agreement. This information should set out the time of delivery where goods not for delivery to third parties are concerned. [37]

There is no doubt that in reviewing their web sites, ordering procedures or advertising methods in order to comply with the requirements of the Distance Selling Directive or the Electronic Commerce Directive (which should be implemented by Member States in the national laws by 17 January 2002), much work is required from e-tailers. As the Distance Selling Directive does not cover financial services, the European Commission made a proposal for a Distance Marketing of Financial Services[38] which would enable consumer protection in the case of distance contracts for financial services. The aim of this Directive is to raise consumer confidence while enabling providers of financial services to market their products in Europe without unnecessary obstacles.

(2) Directive on Electronic Commerce

One of the purposes of the Electronic Commerce Directive is to eliminate barriers which govern the formation and performance of contracts, since a number of rules specific to the physical environment are not appropriate for the e-commerce environment and create concerns regarding the validity and enforceability of electronic contracts.

The Electronic Commerce Directive requires an adjustment of national legislation in order to offer electronic contracts the same recognition as those concluded in a more traditional environment.

The enforcement of the obligation to provide consumers with information requires that Internet service providers supply both consumers and business customers with information regarding on-line contracts.

With the aim of removing legal insecurity when constructing contracts over the Internet, the obligation of information is completed by legal requirements regarding the rule of evidence in the conclusion of the contract. In order to ensure better protection of consumers, the Directive imposes some restrictions on the use of unsolicited commercial communications.

The Electronic Commerce Directive leads to an enhanced understanding of Cyber Consumer expectations in the field of online commerce.

b) Electronic Payment Systems

Electronic payment and its legal framework are essential elements in establishing consumer confidence in electronic commerce. Confidence in B2C e-commerce is closely linked to an inexpensive and secure payment system. In this sense, digital cash solutions will have an obvious impact on the commercial dimension of the electronic market. Due to the large areas it covers, digital cash seems to be an attractive

[37] See Article 5

[38] COM(1999)385 final 98/0245 (COD), Amended proposal for a European Parliament and Council Directive concerning the distance marketing of consumer financial services and amending Directives 97/7/EC and 98/27/EC

option for both consumers and e-tailers. We will examine two types of the emerging digital cash systems: (1) smart cards and (2) digital coins.

(1) Smart cards

Smart cards contain a microprocessor chip, which is embedded into bankcards to make smart cards. The capacity of chips to store information will provide the smart card with multiple functions. These range from electronic wallets to transport tickets or access cards.[39] For instance, Bus Eireann, in Ireland, has developed the "Dash" project where they have created a smart card which has four multi-functions : a-transport ticket , payment for small purchases in shops, telephone cards and a car parking pass[40] These smart cards can be programmed to function as an "electronic purse". The programming for an authorised transaction is made by an electronic terminal, giving the consumer the possibility to process data and to control registered data. The functioning of smart cards in electronic transactions is based on the principle of connecting the consumer to a central database via two encryption keys, one of which is detained by the consumer card holder, with the other linked to the bank's computer.

Mondex[41], Proton and VisaCash are some of examples of micro-payment systems which allow consumers to download electronic money from a personal computer via online banking. Mondex, Proton or VisaCash have a variety of functions which can be used in the payment of goods and services starting with the financial transfer between consumer and e-tailer and include customer loyalty schemes.

The benefits of smart cards for the consumer are security, as unauthorised access is prevented by a lock function; convenience, as it is an easy method of payment; flexibility, as smart cards can be used for all kind of purchases although certain limits are set within each country; control on spending within the limits of an existing amount on the card; and international use - the possibility to allow cardholders to use the card when travelling or transferring money abroad. Finally, in comparison with a credit card, a smart card allows consumers an interest free loan.

With regard to e-tailers, the smart cards present certain advantages such as efficiency, as– smart cards negate the need for customer identification; adaptability - as the smart cards are suitable for the e-tailers of all sizes. For instance, in order to use the Mondex cards, e-tailers will need a Mondex compatible terminal, either integrated with existing equipment or an inexpensive stand-alone version. The pocket sized Mondex 'wallet' can itself be used as a hand held point-of-sale terminal, suitable for use in a taxi or on a market stall. [42]

Further advantages of smart cards include the capacity to solve compatibility problems, which means that e-tailers can use a single electronic terminal for all types of cards. In addition, there are lower costs as the use of smart cards does not involve a large investment for e-tailers, apart from staff training and the purchase of an electronic terminal.

In the U.S., consumers seems to be satisfied with existing alternatives such as cheques, credit cards and debit cards which, in comparison with smart cards, already offer consumers considerable benefits under

---

[39] P. Thomas, A.C. Lacoste - " Smart cards and centralised databanks", Venice, 27-30th September 2000, Seminar Paper, p1

[40] Gavin Sutter, Law & Technology Convergence: Electronic Payments Systems, ECLIP EP 27028 16 December 1999

[41] The Mondex Card is an integrated circuit card (ICC), a "smart" card - a normal plastic card with a small microcomputer "Chip" embedded in it. The Card takes the form of an ISO 7816 integrated circuit card - the international standard for IC cards.

[42] http://www.mondex.com

existing federal regulations. [43] Moreover, consumers seem to *"have shown a high degree of rationality in their choice of electronic payment systems, and have stayed away from more risky or less favourable innovations. Regulated electronic payment systems offer incidental attributes such as float), or reversibility in the event of dispute. Consumers may migrate toward regulated systems because they provide these incidental benefits without regard to how well systemic risk issues are managed. But so long as regulators guarantee the provision of both, then consumers can migrate toward the most favourable package of rights and obligations. "*[44]

At the European level, there are a certain number of initiatives aimed at promoting smart cards as a mechanism for enhancing consumers' confidence in the use of e-commerce. For example, the "e-Action Plan-Secure Network and Smarts Cards" prefigure the new strategy of the EU in the field of electronic commerce. This strategy will be oriented towards the promotion of privacy enhancing technologies and proper codes of conduct. It will also include - the promotion and the development of open source software, security platforms for effective "plug and play", as well as a common core of specifications for using smart cards and for ensuring their security.

(2) Digital coins

In the absence of appropriate equipment for smart card on the consumer's computers, digital coins can be an appropriate method of payment for electronic transactions. The digital coin is based on the following principal: the bank provides consumers with the serial number of a coin encrypted with the bank's private key. If the consumer wants to spend the coin, the bank checks the serial number on the list of spent coins and, if the coin has not already been spent, the bank either credits the e-tailer's bank account or provides the e-tailer with a new coin.[45] There are also other opinions considering that digital coins do not imply lower costs and that a new form of "script" needs to be arranged for micro- transactions[46]. There are two main concerns for using digital coins: anonymity of the consumer and online verification.

With respect to anonymity, it is clear that each transaction using a digital coin allows the processing of personal data " *and the bank ends up with a database containing information on all of its customers; as in the credit-card model, the customers have no privacy".*[47] However, anonymity could be preserved by blinded coins which protects the details of the payer but not that of the payee.

---

[43] *Jane Kaufman Winn "Clash of the titans: regulating the competition between established and emerging electronic payment systems"* http://www.smu.edu/~jwinn

[44]Jane Kaufman Winn "Clash of the titans: regulating the competition between established and emerging electronic payment systems" http://www.smu.edu/~jwinn

[45] A. Michael Froomkin, "Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases"Published at 15 U. Pittsburgh Journal of Law and Commerce 395 (1996).

[46] Steve Glassman et al., "*The Millicent Protocol for Inexpensive Electronic Commerce"*, http://HTTP.CS.Berkely.EDU/~gauthier/millicent/millicent.html

Ronald L. Rivest & Adi Shamir, "*Payword & MicroMint: Two simple Micropayment Schemes* "(Nov. 8, 1995), http://theory.lcs.mit.edu/~rivest/RivestShamir-mpay.ps

[47] A. Michael Froomkin, "Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases"Published at 15 U. Pittsburgh Journal of Law and Commerce 395 (1996).

The second concern of the consumer is related to online verification. In e-transaction between e-tailers and consumers, the e-tailer should verify if the coin offered to him has not previously been spent. It is possible to check the coin's digital signature via the public key corresponding to the coin. However, this verification seems to entail delay and expense.[48]

Obviously, the use of digital cash would enable the growth of e-commerce only if banks implementing this electronic system could ensure consumer privacy protection.

2. The existing regulatory framework for electronic payment

A reliable legal framework for these new payment systems will constitute an important factor in the development of e-commerce. While there is not yet specific European Union legislation to regulate electronic payment, there are some Directives[49] which contain provisions regarding these payment systems.

The Distance Selling Directive provides that consumers be allowed to pay by card. In this way, Member States shall ensure that appropriate measures exist to allow a consumer to request cancellation of a payment where fraudulent use has been made of his payment card and, in the event of fraudulent use, to be re-credited with the amount paid.

The secure use of payment instruments constitutes a supplementary concern for the consumer when they purchase over the Internet. The Commission Recommendation 97/489/EC of 30 July 1997 concerning transactions by electronic payment instruments and, in particular, the relationship between issuer and holder responds to a number of major issues related to the contractual relationship between the issuer and the holder of the payment instrument. The Commission Recommendation establishes obligations on information concerning the terms and conditions of payments and the use of electronic payment instruments, as well as on the liabilities of parties involved in a contractual relationship. With respect to the loss or theft of electronic payment instruments, the consumer's liability should be limited. The "price" of his/her liability should not exceed 150 Euro, except where s/he has acted with extreme negligence or has acted fraudulently. After notification, the consumer should no longer be liable for any loss except where s/he has acted fraudulently. It is also recommended that where payment has taken place without the physical presentation or electronic identification of the instrument itself, the consumer should not be liable for any loss.

With respect to the standardisation of payment card systems in order to guarantee access for all electronic cardholders, it would be useful to consider the Commission Recommendation 87/598/EEC of 8 December 1987 on a European Code of Conduct relating to electronic payments. The aim of this Code is to promote security and ease of use for consumers and to enhance greater security and efficiency for both traders and issuers.

---

[48] Stefan A. Brands, Centrum voor Wiskunde en Informatic (CWI), *Off-line Electronic Cash Based on Secret-Key Certificates* 1-2 (1995) (Report CS-R9506) http://www.cwi.nl/ftp/brands/CS-R9506.ps.Z.

[49] - *Directive 97/7 of 20 May 1997 on the protection of consumers in respect of distance contract; Council Directive 87/102/EEC of 22 December 1986 for the approximation of the laws ,regulations and administrative provisions of the Member States concerning consumer credit;- Commission Recommendation 97/489/EC of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder*

Thi- Recommendation set out a series of general principles relating to the contract between issuers (banks) and traders or consumers. These principles concern the respect of privacy of information given by consumers and the right of fair access to the system for traders, irrespective of their size. Obligations related to the relations between issuers and traders include a ban on any exclusive trading clause which requires the trader to operate only one system as well as an obligation on cardholders to take all reasonable measures in order to make a secure payment.

In addition, the terms of the Commission Recommendation 88/590/EEC of 17 November 1988 concerning payment systems and, in particular, the relationship between cardholder and card-issuer are relevant for consumer protection. Its aim is to provide consumers with adequate information concerning the terms of the contract, particularly with regard to fees. The Recommendation stipulates the rights and contractual obligations of consumers and specifies that consumers would be better protected if contracts were made in writing. In this sense, indications should be made on the period of time within which operations will normally be credited, debited or invoiced. Regarding the treatment of contracts, important indications are stipulated regarding the fact that operations authorised by issuing bodies must be recorded in order to allow the possibility of correcting errors.

Furthermore, the Recommendation specifies the moment of the conclusion of the contract and aims to establish the issuer's liability. The contract concluded between the consumer and the issuer of the payment device must take effect after the consumer has received the payment device and after the consumer has received information on the applicable terms of the contract. The liability is incumbent on the issuer for non-execution or erroneous execution of a contracting holder's payment instructions and allied operations and for operations, which have not been authorised by the contracting holder. This is subject to the contracting holder's own obligations in the event of lost, stolen or copied payment devices.

Conclusions:

As a by-product of its "cyberspace" status, electronic commerce is global, encompassing a whole range of B2C relationships which need to be approached with solutions provided at a local level while remaining viable when applied to global issues. Today, the European Union seems to be endowed with a reliable legal framework for consumer protection. A question which remains, however, is enforcement of this protection. This is probably a matter of time and awareness from both parties in the B2C relationship.

Business should realise that enhancing trust in the minds of consumers is more than a question of technology, it is a question of best practice. Best practice starts with the online service of high street banks as well as with the existence of a secure, user-friendly and cost-effective payment system. It also includes the respect of privacy and the use of smart cards as well as enhancing privacy technologies and fair information practice. In sum, only by offering this guarantee of privacy and security will the consumer be assured that, in cyberspace, his/her interests will be protected in the same manner as in a traditional commercial environment.

Cristina Coteanu, Avocat, Member of the Brussels Bar, ccoteanu@philippe-law.be

LLM European Law, LLM International Law, (ULB - Brussels)

MA in International Relations, MA Management(Solvay Business School - Brussels),

BA in Law