IESE Business School
University of Navarra

Working Paper

WP No 586

March, 2005

ETHICAL ASPECTS OF E-COMMERCE: DATA SUBJECTS AND CONTENT

Alejo J. Sison*
Joan Fontrodona**

* Professor Institute for Enterprise and Humanism, University of Navarra
** Professor of Business Ethics, IESE

IESE Business School – Universidad de Navarra
Avda. Pearson, 21 – 08034 Barcelona. Tel.: (+34) 93 253 42 00 Fax: (+34) 93 253 43 43
Camino del Cerro del Águila, 3 (Ctra. de Castilla, km. 5,180 – 28023 Madrid. Tel.: (+34) 91 357 08 09 Fax: (+34) 91 357 29 13

ETHICAL ASPECTS OF E-COMMERCE: DATA SUBJECTS AND CONTENT

Abstract

This paper reflects on the ethical challenges posed by Internet commerce, with special emphasis on those involving the content and users of the information. The paper discusses the main ethical issues in e-commerce such as security, privacy, identity and nonrefutability of transactions. It proposes measures which both governments and the private sector could adopt to address those issues on different levels. Finally, the paper reflects on the creation of value by leveraging trust and proposes two universal principles to be upheld in Internet commerce: online-offline consistency and technological neutrality.

Keywords: Security, privacy, identity, nonrefutability, e-commerce ethics

ETHICAL ASPECTS OF E-COMMERCE: DATA SUBJECTS AND CONTENT

Introduction

"Reality is virtual." Virtual reality –the reality that exists in the form of bits and bytes and is activated by means of electromagnetic energy, with the help of information technology and telecommunications infrastructure (the Internet)– has changed the way we relate to one another. The spread of Internet use has affected science and technology, art and culture, even politics. But above all it has affected the economy and business.

E-commerce is the sale of goods over the Internet. Generally speaking, it takes place when a buyer visits the web site of a seller and makes a purchase. The fact that the product or service is of a kind that cannot be delivered via the Internet (you cannot digitize a sack of cement) does not mean that the activity cannot be described as "electronic commerce". Strictly speaking, though, the payment, too, should be made electronically, by credit card, e-cash or some other means.

E-commerce is not to be confused with e-business. The term "e-business" refers to a particular way of organizing a company, as a far more flexible and informal economic production unit, in terms of its physical infrastructure and employment relations. E-commerce, by contrast, consists of the whole set of activities carried out by the marketing function (product design, price setting, promotion, etc.) and executed via the Internet. We must also distinguish between e-commerce and the "new digital economy", of which e-commerce is only a part, albeit a tremendously important one (Evans & Wurster, 2000).

In order to understand the ethical issues that arise in relation to e-commerce, it is essential to fully appreciate its advantages and disadvantages compared to conventional commerce (The Economist, 2000b).

The type of products that sell best on-line are "low-touch" products, such as books, CDs, and all kinds of computer-related products. Any product or service that can be digitized ("cyber goods") –such as tickets, audiovisual materials, stock market and banking services, insurance, etc.– also sells very well. In contrast, the Web does not seem to be the most appropriate channel for selling "high-touch" products such as apparel and shoes, food, etc.

Let us not forget the two great advantages of the Internet: its distance-collapsing capacity and its simultaneity, allowing interactive communication among users. There is no need to pay high rents for a physical store or warehouse; most operations are computerized and companies can save on wages. It is as if all businesses could set up shop on Main Street,

where shoppers congregate and can walk right into their store. By using electronic payment, the seller does not have to wait for cash.

For the buyers, the main advantage is price: between 9% and 16% cheaper than in bricks-and-mortar stores, according to a study by Professors Erik Brynjolfsson and Michael Smith of MIT (Varian, 2000). Breadth of product and service offering, combined with convenience, are further contributing factors. One drawback, however, is that for some people cheaper prices are only superficially an advantage, as what they get out of shopping is a gratifying social contact. From that point of view, there is no doubt that e-commerce could lead to greater isolation.

The ethical challenges of e-commerce

Basically, the ethical difficulties associated with e-commerce revolve around three issues: privacy and identity, both with reference to the human subject involved in the transaction, and transaction non-refutability (Baum 1998: 65; Suprina 1997: 8-12; Joyanes 1997: 277-281). A fourth issue to be considered is that of "trespass" or "break-ins" into computer networks, web sites, mailboxes, etc. This is best characterized by the term "hacking", in the sense of doing something supposedly difficult with ease and foiling a system's defenses. Hacking is distinct from violations of privacy, however, because the Web is a "public place", an open system. Like a bricks-and-mortar store, an e-commerce site is private property; but access must be open to the public. The site owner cannot bar anyone from entering; otherwise, there would be a danger of illegal discrimination. The mere fact of entering a web site or an e-mail mailbox does not violate the owner's privacy; once inside, however, the visitor may behave inappropriately.

Issues relating to security

Hacking, "cracking" and "page jacking" can be jointly categorized as attacks on a system's security. Security refers to the fact that information is stored and transmitted exactly as the system owner originally intended (KPMG 2001: 3). As a rule, computer security systems are designed so that information and transactions carried out via the system are kept private, although they may also be designed to ensure the opposite – in other words, to ensure that employees do not have privacy in their workplace, for whatever reasons. Without a proper security system, it will be impossible to achieve privacy in an organization.

Hacking is an attack on the computer itself, be it a particular PC or the entire network, as a data store and communication medium. It jeopardizes the confidentiality, integrity or availability of the information stored on the computer, or the services it provides (US Department of Justice 2000: 10). Previously, as a pastime for computer-savvy adolescents and others, hacking was not necessarily a criminal activity. Often, it was done to play a tiresome joke on the owner or administrator of the targeted computer system by "cracking" its secret access codes. As a form of protest, hackers would sometimes "hijack" a web site ("page-jacking") and redirect would-be visitors elsewhere.

More recently, however, malicious hacking has become more common. Such, allegedly, was the case of Jeffrey Hirschorn, a reporter for IPO.com, a news company that covers the launch of new stocks on the New York stock exchange (Bloomberg News 2000). Initially, Hirschorn worked for IPO.com's rival, Wall Street Source. Then, in September 1999, Wall Street Source dismissed him in what Hirschorn claimed was an act of anti-Jewish discrimination. Some months later, now working for IPO.com, Hirschorn allegedly used the

password of a part-time employee at Wall Street Source to break into the company's computer system and deleted data from its web site. As a consequence, Wall Street Source was forced to revamp its entire security system. In May 2000, Wall Street Source filed a suit against Hirschorn and IPO.com for sabotage, seeking $100,000 in compensatory damages and $5 million in punitive damages.

The ethically questionable practices of hackers can be categorized in three types: theft of confidential information, theft of services, and sabotage of the information network.

Firstly, theft of information from confidential files. The preferred targets are government computers. The computer systems of private institutions and corporations are also liable to this type of attack. For example, a hacker may break into a hotel booking system to steal credit card details. It could also be done in order to steal various kinds of "intellectual property": from trade secrets to copyrighted materials such as computer software. Lastly, a hacker may engage in "cyber harassment": obtaining confidential information about a person in order to practice extortion or satisfy an unhealthy curiosity (US Department of Justice 2000: 12). Computer systems used to store clinical histories, credit histories, telephone numbers and addresses, etc. are especially vulnerable.

Secondly, theft of services. Hackers may break into a computer system in order to control the operations it regulates and use services without paying for them, or sell them on to others. There have been intrusions into telephone systems, for example, to make "free" calls, or into computers in order to decipher keys and PINs of ATM cards.

Thirdly, hackers may cause damage by swamping a PC, server, or part of a network: for instance, with "denial of service" attacks (The Economist 2000a; Sager *et al.* 2000). This may be done by "mailbombing", that is, by sending a flood of e-mail messages to a target account, causing an overload. All the hacker has to do is copy a small program and install it on various computers, or better still, on the computers of an Internet Service Provider (ISP). This was the technique employed to put the largest on-line shopping sites, such as Yahoo, Amazon, e-Bay and Buy, out of action in February 2000. Deliberately interrupting the services of a computer network is a federal crime in the United States, and carries a maximum sentence of five years in jail and a fine of $250,000 dollars plus damages (Bonner 2000).

Computer networks may also be brought down by the spread of "viruses" and "worms". Worms differ from viruses in that they not only reproduce but also are capable of re-sending themselves across the network (Markoff 2000b). The "Melissa" worm cost users around the world some $80 million in lost time, effort, data and business opportunities (Markoff 1999b). In May 2000, the "I love you" bug may have caused up to $10 billion worth of damage (Reuters 2000a).

Currently, wireless Internet access has added further sophistication to hackers' perverse activities. The fact that companies allow their employees to access their central computers from outside their workplace makes the hackers' job easier.

Issues relating to privacy

On-line advertising can be extraordinarily precisely targeted thanks to "cookies", which are small text files that companies install on the hard drives of people who visit their sites in order to be able to track visitors' browsing habits. With the help of these cookies, advertising agencies are able to build up a profile of each user, including, for example, the sites he/she visits most, how long he/she spends at each site, the date of his/her last visit, etc. (Green, Alster & Borrus 2000).

On January 27, 2000, Harriet Judnick, an administrative assistant from California, filed a lawsuit against DoubleClick alleging violation of privacy rights and deceptive business practices. In November 1999, DoubleClick had paid $1.7 billion for Abacus Direct, a conventional direct marketing company. Abacus Direct had large databases containing records of customers' catalog purchases. According to Judnick, DoubleClick had changed its marketing policy: the information about Web surfers that previously it had gathered anonymously was now going to be combined with actual names and addresses, thanks to the data owned by Abacus Direct. That meant that DoubleClick would know the name, postal address, telephone number and other information about the Internet users whose online profiles it had built up using cookies. Judnick believed that DoubleClick was trading in personal information without the knowledge or consent of consumers. Although clearly this would be nirvana for direct marketers, it would be a nightmare for anyone who wanted to protect his/her privacy.

In view of the avalanche of criticism, DoubleClick decided to back down. The company's CEO, Kevin O'Connor, admitted having made a mistake in planning to merge names with anonymous web user activity in the absence of clear ethical and legal standards (Seglin 2000). These events were sufficient to spark an intense public debate about on-line privacy protection against "data mining" or "data profiling" companies (Clausing 1999).

Privacy is desirable insofar as it allows a person to reaffirm his/her individuality, set him/herself apart from the group and lay claim to his/her own space or domain. Privacy is defined as protection of the collection, storage, processing, dissemination and destruction of personal information (KPMG 2001: 3). "Personal information" is understood to mean any information about an identifiable individual or institution (name, address, telephone number, social security/insurance or other government identification number, employer, credit card number, personal or family financial information, personal or family medical information, etc.). Some information is known as "sensitive information", insofar as it may be used to make discriminations prohibited by law.

The problem of privacy in e-commerce concerns the difficulty of securely conveying the information required for on-line transactions (Suprina 1997). The aim is to ensure that whatever information is sent is not intercepted by anyone other than the person for whom it is intended. Protecting the privacy of communication is a great challenge, due to the very nature of the on-line medium, an open network of digital telecommunications. It is technically and economically impossible to patch all the holes through which unauthorized intruders may gain access (Coleman 1999a). As experience has shown, those determined to violate the privacy rights of Internet users are becoming increasingly ingenious in their methods (Garfinkel 1999; The Economist 1999c; Rosen 2000). There is no such thing as absolute privacy; efforts should be directed instead toward obtaining the appropriate degree of privacy, as agreed by all parties, for each type of transaction (The Economist 1999b).

There are three types of privacy protection measures:

1) measures pertaining to the physical structure or configuration of the network, such as building "firewalls" into computers and information and telecommunications systems (Stewart 1998). The task is to decide, with privacy as a criterion, what computer hardware should be installed in what networks (LAN, intranet, public Internet), and control access to each one (fixed or mobile telephone connections, ISPs, portals), while avoiding insecure "back doors" (Freedman 1999). The best ally of privacy is still physical separation, combined with the absence of cables, aerials, infrared portals or receivers of any kind of electromagnetic energy through which digitized information may pass.

2) measures using protocols or software applications, of which there are two types: first, passwords and PINs; and second, cryptography.

3) measures based on ethical and legal rules of behavior. On the one hand, these are the measures that offer the weakest guarantees; on the other, they may be the most effective, as respect of privacy and violation of privacy are both, after all, human, not electronic, acts. The goal, therefore, is to reach agreement on appropriate criteria for action: what behaviors should be prohibited, avoided, permitted, encouraged, and why (Nail, Prince & Schmitt 2000).

Public sector initiatives in the U.S. began with the "Code of Fair Information Practices" of 1973, and the "Privacy Act" of 1974 (KPMG 2001:8). The "Code of Fair Information Practices" of 1973 established five universal principles for the use of databases and computer systems:

1) Organizations may not maintain personal data record-keeping systems whose very existence is secret.

2) An individual must be able to find out what personal information is in a record and how it is used.

3) An individual must be able to prevent personal information that was obtained for one purpose from being used or made available for other purposes without his/her consent.

4) An individual must be able to correct or amend a record of personally identifiable information.

5) Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

For its part, the "Privacy Act" regulates the collection and use of personal information by federal government agencies.

This body of U.S. practices was subsequently adopted by the OECD in its "Guidelines for the Protection of Personal Data and Trans-border Flows of Personal Data" of 1980. These guidelines were reaffirmed for application to the Internet in the report "Implementing the OECD Privacy Guidelines in the Electronic Environment", published in 1998. That same year, a European rule came into force whereby companies could only convey information about EU consumers to countries in which the information would have the same level of protection as it has within the EU. The U.S. –where legislation on this subject has been put on ice and self-regulation has prevailed– is excluded from this safe area (Stewart 1998: 2). This EU policy brought loud protests from United States companies, with the more belligerent among them threatening to take the matter to the World Trade Organization, as an unlawful discriminatory measure. In July 2000, the United States' credibility in matters of privacy protection took a serious blow when it was discovered that the FBI had installed surveillance systems, such as the one known as "carnivore", on the networks of various Internet service providers (Reuters 2000b).

The report on the state of on-line privacy in 2003 submitted by the U.S. Federal Trade Commission underlined the importance of introducing more consumer-oriented

legislation. At the same time, self-regulation was chosen as the means to ensure protection of consumer privacy and underpin the growth of the on-line market.

Since October 2002, Spain has had a "Law of Information Society Services and Electronic Commerce" (LSSI). The LSSI establishes a regulatory framework for information society services and e-commerce, setting out the obligations of service providers. It formulates rules for validity and effectiveness, and the sanctions applicable to information society service providers.

One of the subjects regulated by this law is the sending of unsolicited e-mail advertising, or "spam". The law stipulates that Information Service Providers who need to know their customers' e-mail addresses must give their customers the option not to receive advertising messages, and if the customers have agreed to receive such messages, they must also have the option to reverse their decision at no cost to themselves. It should be mentioned, however, that the 1999 Organic Law on Data Protection allows a loophole for the sending of "spam", insofar as it permits the collection of addresses and other personally identifiable information from public sources.

The private sector has launched a number of initiatives to bolster on-line privacy. The World Wide Web Consortium (W3C), an international body that develops Internet protocols, has proposed the "Platform for Privacy Preferences" (P3P), a set of technical specifications that allows consumers to choose and decide what information about themselves they want to reveal and, to some extent, control how it is used (Stewart 1998: 2-3). Other initiatives have included the creation of independent, non-profit organizations to monitor compliance with agreements on the confidentiality of consumer data. Businesses sign agreements with these organizations, the best-known of which is Trust-e, and pay them a fee in return for the right to display the organization's privacy seal or "trustmark" on their web site.

In April 1999, the Spanish Advertising Self-Regulatory Association (AAP) drew up –following EU rules– an ethics code for on-line advertising (ABC 1999a). This voluntary code was the first of its kind in Europe and can be summed up in the following ten points:

1) The advertisement and the advertiser must identify themselves.

2) Current data protection laws must be obeyed.

3) Children under the age of 18 may not submit information to a web site without parental authorization.

4) Advertising content aimed exclusively at adults must be identified.

5) Children under the age of 18 must not be directly encouraged to buy a product or service.

6) E-mail advertising is not allowed unless it has been solicited by the recipient (anti-spam).

7) Newsgroups may not be used to gather data for advertising purposes.

8) Advertising on the World Wide Web must not prevent users from surfing freely.

9) If advertising interruptions are unavoidable in order to access a site's editorial content, the user must be warned of that fact.

10) Sponsoring web sites must be identified.

In 2000, the AAP and the Spanish E-Commerce Association (AECE) decided to join forces to establish a comprehensive system of self-regulation for interactive advertising and e-commerce. With the collaboration of the Interactive Advertising Bureau Spain (IAB Spain), they produced the current "Ethics Code of E-Commerce and Interactive Advertising".

This code can be summed up as follows:

- Advertising in electronic media must be designed and produced with a sense of social responsibility.
- On-line advertising must not contain content that offends the dignity of the person, or that is discriminatory.
- The advertiser must identify itself, so that recipients of the advert know who is responsible for it and are able to contact the advertiser without difficulty.
- The advertising must be easily identifiable as such, all types of hidden advertising being prohibited.
- Advertisers must inform clearly about the cost of accessing a message or service when that cost is greater than that of basic telecommunication services, and they must do so before the user accesses the service.
- Advertising offers must be identifiable, so that the recipient is able to recognize them for what they are.
- Advertising promotions in electronic communication media must adhere to the rules governing advertising in general, especially those of legality, truthfulness and good faith.
- Advertisers must respect intellectual and industrial property rights and avoid unfair competition.

Furthermore, Internet service providers belonging to the Cross-Industry Association of Spanish Electronics Companies (Asimelec) have produced their own code of conduct, in which they take a stand on issues such as child pornography (ABC 2000). What is missing from that document, however, is a balance between providers' control over and responsibility for on-line content, on the one hand, and the need to safeguard users' freedom of expression and freedom of the press, on the other.

Accepting that privacy can never be absolute and that the precise degree of privacy appropriate to any given virtual transaction will depend on many different factors, criteria must be established to help reduce conflicts of interest between privacy and other relevant interests in the on-line market. It is recommended that the following principles be observed (Green, Alster, Stepanek & Borrus 2000):

1) Notification. Companies must notify users, on their web sites, whether or not they collect user information, what they use it for and who will have access to it.

2) Opt-out. Consumers must be able to control the collection and use of their personally identifiable information; therefore, they must be given the option to opt out of the collection, transfer and sale of their personal information.

3) Access. Consumers must be able to access the files that companies keep with consumers' personal information in order to verify that information, correct any errors, erase any details they disagree with, etc.

4) Security. Companies must assume responsibility for the security of the data they collect; and if they fail in that task, they must be sanctioned accordingly.

Issues relating to identity

Neither anonymity nor its opposite, identity verification, are absolute values. Depending on the type of transaction, users may prefer anonymity: take the purchase of medicines, for example (US Department of Justice 2000: Appendix D, Internet Sale of Prescription Drugs and Controlled Substances), and the interest that insurance companies might have in gaining access to that information. It is appropriate for pharmacies to sell their products anonymously. By contrast, when an order is given to buy stocks, both the customer and the broker will do well to verify the "virtual" identity of the other party.

Computers have serious limitations when it comes to establishing a user's identity, given that identity is a personal, physical characteristic. A baby that cannot even talk, or a toddler, is more reliable when it comes to identifying its parent than the most powerful computer. At best, a computer can detect that a person expresses him/herself or behaves in accordance with certain empirically verifiable characteristics; but it cannot know or recognize personal identities. This shortcoming of computer systems is what makes "identity theft" possible.

Identity theft or impersonation can occur in a variety of ways. When a person makes a purchase with a credit card, all the shop assistant has to do is scan the card twice, once with the cash register and again with any digital card reader, in order to be able to subsequently charge items to that person's account (Wells 2000). With the information available in many databases, it is possible to open new credit card accounts, telephone accounts, etc. (O'Brien 2000). Such fraudulent transactions are made easier by the fact that, sadly, for many companies nowadays the customer is no more than a credit card; every last vestige of a personal relationship has disappeared. On the one hand, we appreciate the convenience of being able to shop on-line without having to go to the store in person; on the other, perhaps unwittingly, we expose ourselves to the danger that someone will impersonate us by stealing our identity (Slade 2000).

The tension between identity and anonymity is reflected in the following examples. As is common practice among mass manufacturers, Microsoft and Intel use a "global unique identifier" for their products. It helps them to control their inventories and to know, for example, which batch must be withdrawn if a defect is detected. Several consumer groups have complained about this feature of Microsoft's Word software and Intel's microchips, because they consider that the electronically readable number compromises their on-line anonymity (Markoff 1999a; CNET News.com 2000). Nonetheless, thanks precisely to that unique number, cyber-sleuth Richard Smith was able to help the police locate and identify the presumed creator of the Melissa virus (Markoff 2000a).

Those in favor of anonymity advocate the use of alternatives to the conventional personal credit card. These include e-cash, digital cash, and electronic purses or smart cards, especially for micro-payments (Stewart 1998: 13-15). For the time being, however, none of these systems –Secure Electronic Transactions (SET) coupled to credit cards, CyberCash, or First Virtual– have been able to win consumers' confidence, not only because of the practical

and technical difficulties but also for theoretical or economic reasons: they seem to demand a whole new "monetary and financial policy" on the part of companies and nations (The Economist 1998: 2000b). Moreover, although e-cash is protected by high-level security systems, it is not impregnable; and once its secret code has been deciphered, as happens sooner or later with all digital information, the "copy" or "forgery" becomes indistinguishable from the original: cash has been converted into software (Roddy 1999: 14-15).

Lastly, another concern regarding anonymity is the fact that the Internet offers opportunities for money laundering. Although this danger has been much talked about in connection with certain banking practices and the complicity of "tax havens", the fact is that every international bank transfer necessarily goes through one of two electronic systems, CHIPS or SWIFT, whose basic organization is located in the United States (Helleiner 1999). Accordingly, there is little to stop the United States government from intervening, if it so wishes, and obtaining information about the source and destination of large capital flows. There will always be "digital fingerprints" to be found by those who have the resources and the patience to hunt for them; which means that it is best to behave on-line as if there were no anonymity.

Issues relating to non-refutability

On April 7, 1999, on what appeared to be a page belonging to the Bloomberg financial news agency's web site, a report appeared to the effect that an Israeli company was about to buy the U.S. telecommunications equipment manufacturer PairGain (The Economist 1999a). This triggered a buying spree that pushed the price of PairGain stock up from $8.50 to $11.13 per share. It would have been a great opportunity to make money, if it hadn't been for the fact that the story was a fabrication: somebody had copied Bloomberg's masthead and had spread the false rumor across the Web. It is not even necessary for a hoaxer to pass him/herself off as somebody else by copying a masthead or any other emblem; all he/she has to do is go to a chat group or bulletin board and sow rumors. The effort required to publish stories on the Internet is minimal, and false news can spread like wildfire, reaching huge audiences. The damage that can be caused is out of all proportion to the effort.

Non-refutability is a property that makes it possible to verify what really happened (Suprina 1997). In e-commerce, that is usually done by keeping time-stamped records of all transactions between the parties. In case of doubt, the relevant files can be retrieved from the archive to confirm the validity of an agreement. It is hoped that this will help to resolve or, better still, prevent the tens of thousands of cases of on-line fraud reported in 1999 (Clausing 1999).

Because on-line transactions tend to be fast and fluid –a mouse click is all it takes– and are not documented on paper, a person may always claim there was a mistake or confusion when giving his/her consent. On-line communication is too easy and mechanical, and we do not always sufficiently appreciate the implications and consequences of our acts (Lloyd 2000).

We have already talked about cryptographic techniques, with public and private keys to encode and decode messages. This technology can be used not only to safeguard privacy and confidentiality, but also to verify the "identity" of the parties to a transaction (Coleman 1999b).

"Digital signatures" have been invented to ensure non-refutability: they not only protect documents from tampering, but also authenticate their source and origin. Various electronic technologies can be used to create "digital signatures", from the scanning of a

handwritten signature to the digitization of unique biometric measures such as a person's fingerprints, an image of the retina, etc. Subsequently, a "digital certificate" issued by a trusted third-party authority –such as VeriSign or Entrust– may be used to authenticate the signature, as a further security measure: This is the equivalent of an electronic notarial seal (Stewart 1998: 9-12; Ray 2000).

In September 1999, the Spanish government approved a law on digital or electronic signatures, anticipating moves by the European Union and the United States (ABC 1999b). Both public and private bodies may offer a signature certification service as "impartial third parties". Since then, this new legislation has had major social repercussions as a legal basis for electronic data exchange (Sigüenza 2000: 16-20; Alamillo 2000: 22-26).

In 2004, almost half a million people (446, 239) used electronic signatures. The advantages of electronic signatures are that they reliably identify the sender of a message, verify whether or not a document has been tampered with, and ensure that sender and recipient cannot deny each other's existence.

Although in Spain electronic signatures can only be used to pay taxes and communicate with government institutions, "there exists the possibility" of extending their use to private e-commerce, because "it is technically possible and, legally speaking, it offers additional security, which is its main value" (Belt Ibérica S.A. 2004).

In the physical world, three conditions are usually required for a contract to be legally valid: it must be in writing, the written document must be the original, and it must be signed by both counterparties. In the virtual world of e-commerce, the best we can hope for is an approximation to those prerequisites. Sometimes, the degree of approximation is insufficient, and so disputes arise.

However much a "virtual contract" resembles a "physical contract", they are not the same thing. That is why companies tend to use paper contracts, even if they have already reached a virtual agreement. And yet, doing so negates one of the main advantages of e-commerce. Often, disputes over virtual contracts never go to court because the amounts involved are insignificant. But if lawsuits are filed, many important questions of law will need to be decided: Who has jurisdiction in cyberspace? What type of law is applicable to such disputes? To what extent must the decisions of foreign courts be respected?

Conclusion

When e-commerce came into being, it promised to bring us much closer to the conditions of a fully efficient market. Never before had so many sellers been brought together with so many buyers, with the possibility of instantaneously exchanging so many products and services. Once again, however, we have had to acknowledge that there is no such thing as perfection, not even in the virtual world. And the specific factor that has let us down in this case has been, primarily, information. And when we say information, we also necessarily mean trust, because the one depends on the other. Of course, the information we require about products and prices is right there, readily accessible on the Web; but still it is difficult for us to gather it all and have it at our fingertips at the crucial moment when we issue a judgment and make our decision (Hagel & Singer 1999).

Clearly, the growth of e-commerce will create new challenges in our efforts to safeguard consumers' privacy, identity and anonymity, as well as the integrity and reliability of their commercial transactions. But, as has been demonstrated, none of those values can be

taken as absolutes; they have varying degrees of importance, depending on a range of circumstances. Accordingly, they belong in the sphere of prudential judgment.

With respect to private decisions, agents may act on three fronts: the physical information infrastructure (hardware), the specialized applications (software), and above all, the proper training of buyers and sellers alike in the rules of "netiquette". Success in such initiatives will minimize the need for government regulation (Tagliabue 2000).

Besides this three-pronged approach, we propose two general principles that should serve as guidelines for any debate on the ethics of e-commerce.

First, the principle of "on-line/off-line consistency" when it comes to evaluating behavior. The basic ethical and legal standards that govern human conduct in the physical world apply equally in cyberspace. The Web cannot and must not become a sanctuary for unscrupulous operators acting in ways that would be considered illegal and immoral in the physical world. Conversely, conduct that is not prohibited in the physical world –such as expressing opinions contrary to the "official" view on whatever subject– must not be banned simply because it takes place in the virtual world (Blázquez 2000:324-327).

The principle of consistency of standards highlights the importance of a second principle, almost a corollary of the first, which is that of "technological neutrality". Nothing that the networked devices do "by themselves" has any ethical significance independently of the actions of a human agent and the intention inherent in those actions.

There have always been those who have claimed to see a conflict between market efficiency and the ethical value of people. In our view, however, the main ethical value of e-commerce lies precisely in the fact that increased market efficiency works ultimately to the benefit and greater well-being of people. The increase in market efficiency translates into more, better and cheaper products for all consumers: a better quality of life.

As Sen (1999) recently reminded us, the more efficient a market is, the freer the agents will be to make better economic decisions that foster greater well-being. Without a doubt, freedom of the market –like freedom of expression, to mention another example– brings with it problems of its own in the form of possible abuses; but it is infinitely better to run those risks than to pre-emptively suppress freedom out of fear of the consequences.

References

ABC 1999a: “Autocontrol redacta el primer código ético sobre publicidad en Internet de Europa”, April 16.

ABC 1999b: “La firma digital, clave para los nuevos servicios que vienen”, October 3.

ABC 2000: “Proveedores de servicios de Internet se dotan de un Código Deontológico”, April 7.

Alamillo, I. 2000: “La firma electrónica en el departamento financiero”, *Banca & Finanzas*, no. 53, March.

Baum, D. 1998: “Internet Security: Building a Safe Ride”, *Oracle Magazine*, January/ February.

Blázquez, N. 2000: *El desafío ético de la información*, Salamanca/ Madrid, San Esteban/ Edibesa.

Bloomberg News 2000: “Reporter Accused of Hacking Into Rival’s Computer”, *New York Times*, May 5.

Bonner, R. 2000: “Web Attacks Have Government Reviewing Laws and Security”, *New York Times*, February 11.

Clausing, J. 1999: “FTC Asked to Examine Data-Profiling Practices”, *New York Times*, November 9.

Clausing, J. 2000: “Government Fights Spread of Online Auction Fraud”, *New York Times*, February 15.

CNET News.com 2000: “Intel to Phase Out Processor Serial Numbers Attacked by Privacy Advocates”, *New York Times*, April 28.

Coleman, A. 1999a: “The Changing Security Paradigm”, *Sun Journal*, 3-2.

Coleman, A. 1999b: “Authenticating Identities Online”, *Sun Journal*, 3-3.

The Economist 1998: “Keep the Change”, November 21.

The Economist 1999a: “Gossip on the web. Truth, lies and cyberspace”, April 24.

The Economist 1999b: “The End of Privacy. The Surveillance Society”, May 1.

The Economist 1999c: “Living in a global goldfish bowl”, December 18.

The Economist 2000a: “Anatomy of an attack”, February 19.

The Economist 2000b: “Define and sell”, February 26.

Evans, P. & Wurster, T. 2000: *Blown to Bits. How the New Economics of Information Transforms Strategy*, Boston, Harvard Business School Press.

Freedman, D. 1999: “Top Secret but Easily Stolen”, *New York Times*, May 10.

Garfinkel, S. 1999: *Database Nation: The Death of Privacy in America*, Sebastopol, CA, O’Reilly.

Green, H., Alster, N. & Borrus, A. 2000: “Privacy Outrage on the Web”, *Businessweek*, February 14.

Green, H., France, M., Stepanek, M. & Borrus, A. 2000: “Online Privacy. It’s Time for Rules in Wonderland”, *Businessweek*, March 20.

Hagel, J. & Singer, M. 1999: *Net Worth. Shaping Markets When Customers Make the Rules*, Boston, Harvard Business School Press.

Helleiner, E. 1999: “Sovereignty, Territoriality, and the Globalization of Finance”, in *States and Sovereignty in the Global Economy* (A. Smith, D.J. Solinger & S. Topik, eds.), London, Routledge.

Joyanes, L. 1997: *Cibersociedad. Los retos sociales ante un nuevo mundo digital*, Madrid, McGraw-Hill.

KPMG 2001: *A New Covenant With Stakeholders: Managing Privacy as a Competitive Advantage*, KPMG LLP.

Lloyd, N. 2000: “You Paid That Bill with a Single Click. Or Did You?”, *New York Times*, July 2.

Markoff J. 1999a: “Intel Goes to Battle as Its Embedded Serial Number is Unmasked”, *New York Times*, April 29.

Markoff, J. 1999b: “Guilty Plea Expected in Virus Case”, *New York Times*, December 9.

Nail, J., Prince, F. & Schmitt, E. 2000: “Privacy Self-Regulation Goes Poof”, *The Forrester Brief*, March 16.

O’Brien, T. 2000: “Aided by Internet, Identity Theft Soars”, *New York Times*, April 3.

Ray, T. 2000: “Sign of the Times”, *New York Times Magazine*, July 2.

Reuters 2000a: “Insurers Unlikely to Pay for Virus Damage”, *New York Times*, May 6.

Reuters 2000b: “Justice Department Releases Guidelines for Carnivore Review”, *New York Times*, August 24.

Roddy, D. 1999: *The New Economics of Transactions. Evolution of Unique e-Business Internet Market Spaces*, Deloitte Touche Tohmatsu.

Rosen, J. 2000: “The Eroded Self”, *New York Times Magazine*, May 5.

Sager, I., Hamm, S., Gross, N., Corey, J. & Hoff, R. 2000: “Cybercrime”, *Businessweek*, February 21.

Seglin, J. 2000: “Who Is Minding Your Business?”, *New York Times*, March 19.

Sen, A. 1999: *Development as Freedom*, Oxford/ New York, Oxford University Press.

Sigüenza, F. 2000: "Impactos del documento electrónico en el departamento financiero", *Banca & Finanzas*, no. 53, March.

Slade, M. 2000: "On the Global, Faceless Web, Trust Counts for Even More", *New York Times*, March 29.

Stewart, T. 1998: *Selected E-Business Issues. Perspectives on Business in Cyberspace*, Deloitte Touche Tomatsu, September.

Suprina, D. 1997: "Privacy, Identity and Non-Refutability: Requirements for Digital Age Applications", *Sun Journal*, 1-3.

Tagliabue, J. 2000: "Creative Web Taxes in Europe", *New York Times*, September 28.

US Department of Justice 2000: "The Electronic Frontier", March.

Varian, H. 2000: "Online Commerce Creates Strange Competition", *New York Times*, August 24.

Wells, S. 2000: "When It's Nobody's Business but Your Own", *New York Times*, February 13.